

**Builders-2020-03-12**

# 소개 및 목차

## TransitGateway

### TransitGateway Overview

Transit Gateway에 대한 전반적인 내용을 소개합니다.

### TransitGateway 구성하기

Multi VPC 환경에서 Transit Gatway 구성과 North-To-South, East-To-West 트래픽의 제어와 연결에 대해서 소개합니다.

### TransitGateway MultiAccount

동일 리전의 멀티 어카운트 환경에서 RAM을 이용한 TGW공유 방법을 소개합니다.

### TransitGateway Peering

서로 다른 리전에서 TGW간 Peering 방법을 소개합니다.

### TransitGateway Monitoring

Transit Gateway 구성 완료이후 모니터링에 대한 방법을 소개합니다.

---

## Gateway Load balancer

### GWLB Overview

---

# Network Firewall

## Network Firewall Overview

해당 LAB의 질문 사항은 whchoi98@gmail.com/ whchoi@amazon.com 또는  슬랙채널 (<https://whchoi-hol.slack.com/archives/C01QM79Q4BD>)에서 문의 가능합니다.

시작에 앞서

# 사전 준비

## 사전 준비 사항 및 도구 소개

- 키 페어
- Cloud9 구성 - EC2 인스턴스 접속과 yml 수
- System Manager & Session Manager (랩에서 Cloudformation으로 자동배포 합니다.)

랩 시작에 앞서 다음과 같은 사전 준비를 합니다.

모든 EC2 인스턴스 콘솔은 Cloud9 또는 Session Manager를 통해서 접속합니다. 따라서 Cloud9과 System Manager - Session Manager가 반드시 필요합니다.

System Manager와 Session Manager는 Cloudformation 기반의 Yaml을 통해 모두 사전 구성되어 있습니다.

Cloud9은 비용이 별도로 부과되지 않은 Cloud 기반의 IDE 콘솔 도구입니다.

## 키 페어 만들기

AWS 관리 콘솔 - EC2 - 네트워크 및 보안 - 키 페어 - 키페어 생성 을 선택합니다.

### ▼ 네트워크 및 보안

보안 그룹 [New](#)

탄력적 IP [New](#)

배치 그룹

### 키 페어

네트워크 인터페이스 [New](#)



아래와 같이 키페어 이름을 입력합니다. 해당 키 페어는 이름을 동일하게 합니다.

builders20210312

파일 형식을 pem 을 선택하고, 키 페어 생성 을 클릭합니다.

EC2 > 키 페어 > 키 페어 생성

## 키 페어

프라이빗 키와 퍼블릭 키로 구성되는 키 페어는 인스턴스에 연결할 때 자격 증명을 증명하는 데 사용하는 보안 자격 증명 세트입니다.

이름

이름에는 최대 255개의 ASCII 문자가 포함됩니다. 앞 또는 뒤에 공백을 포함할 수 없습니다.

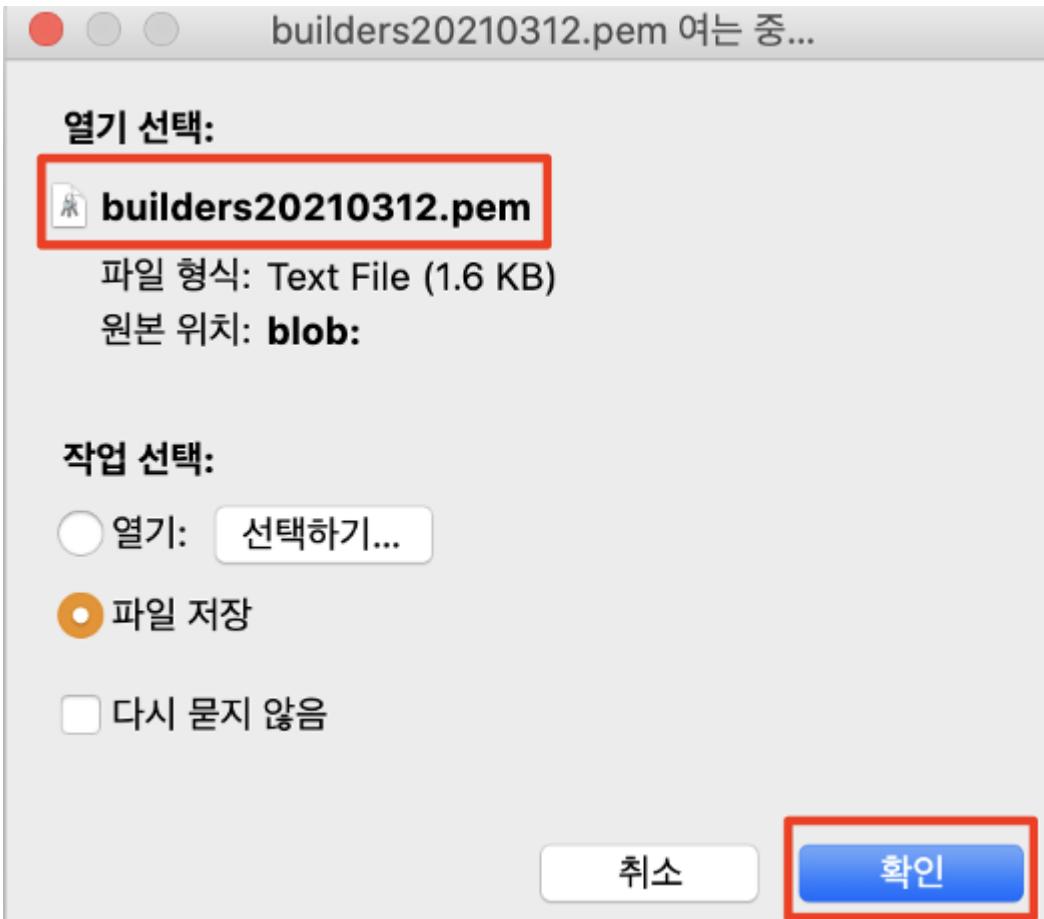
파일 형식  
 pem  
OpenSSH와 함께 사용

ppk  
PuTTY와 함께 사용

태그(선택 사항)  
리소스에 연결된 태그가 없습니다.

태그를 50개 더 추가할 수 있습니다.

생성되면 pem key를 로컬 PC에 다운 받습니다. (저장 경로는 각 운영체제의 기본 다운로드 폴더입니다.)



AWS 관리 콘솔 - EC2 - 네트워크 및 보안 - 키 페어 을 선택하고 정상적으로 만들어 졌는지 확인합니다.

키 페어 생성 완료	
키 페어 (2)	
<input type="button" value="C"/> <input type="button" value="작업"/> <input type="button" value="키 페어 생성"/>	< 1 >
<input type="text" value="키 페어 풀터입력"/>	
□ 이름	▼ 지문
builders20210312	4f:96:af:fe:9b:dd:4e:16:5a:a7:99:cf:c7:57:8f:b... key-01bc59e317dd4e90f

-  해당 키페어 이름은 다음 실습에서 Cloudformation에 이미 binding 되어 있습니다. 다르게 할 경우에는 Cloudformation 진행과정에서 다시 선택해도 됩니다.

## Cloud9 구성

# Cloud9 소개

AWS Cloud9은 브라우저만으로 코드를 작성, 실행 및 디버깅할 수 있는 클라우드 기반 IDE(통합 개발 환경)입니다. 코드 편집기, 디버거 및 터미널이 포함되어 있습니다. Cloud9은 JavaScript, Python, PHP를 비롯하여 널리 사용되는 프로그래밍 언어를 위한 필수 도구가 사전에 패키징되어 제공되므로, 새로운 프로젝트를 시작하기 위해 파일을 설치하거나 개발 머신을 구성할 필요가 없습니다. Cloud9 IDE는 클라우드 기반이므로, 인터넷이 연결된 머신을 사용하여 사무실, 집 또는 어디서든 프로젝트 작업을 할 수 있습니다. 또한, Cloud9은 서비스 애플리케이션을 개발할 수 있는 원활한 환경을 제공하므로 손쉽게 서비스 애플리케이션의 리소스를 정의하고, 디버깅하고, 로컬 실행과 원격 실행 간에 전환할 수 있습니다. Cloud9에서는 개발 환경을 팀과 신속하게 공유할 수 있으므로 프로그램을 연결하고 서로의 입력 값을 실시간으로 추적할 수 있습니다.

## 장점 소개

### 실시간으로 함께 코딩

AWS Cloud9를 사용하면 코드 협업이 쉬워집니다. 클릭 몇 번으로 개발 환경을 팀과 공유하고 프로그램을 함께 연결할 수 있습니다. 협업을 진행하는 동안 팀원은 서로 입력하는 것을 실시간으로 보고 IDE 내에서 바로 채팅할 수 있습니다.

### 손쉽게 서비스 애플리케이션 구축

AWS Cloud9을 사용하면 서비스 애플리케이션을 손쉽게 작성, 실행 및 디버깅할 수 있습니다. AWS Cloud9은 서비스 개발에 필요한 모든 SDK, 라이브러리 및 플러그인으로 개발 환경을 사전에 구성합니다. 또한, Cloud9은 AWS Lambda 함수를 로컬에서 테스트하고 디버깅 할 수 있는 환경을 제공합니다. 코드에 직접 반복할 수 있으므로 시간을 절약하고 코드 품질을 개선할 수 있습니다.

### 터미널에서 AWS에 직접 액세스

AWS Cloud9에는 사전에 인증된 AWS 명령줄 인터페이스와 더불어 개발 환경을 호스팅하고 있는 관리형 Amazon EC2 인스턴스에 대한 sudo 권한이 포함된 터미널이 함께 제공됩니다. 따라서 명령을 신속하게 실행하고 AWS 서비스에 직접 액세스할 수 있습니다.

### 새로운 프로젝트를 신속하게 시작

AWS Cloud9를 사용하면 새로운 프로젝트를 손쉽게 시작할 수 있습니다. Cloud9의 개발 환경은 Node.js, JavaScript, Python, PHP, Ruby, Go 및 C++를 비롯한 40여 개의 프로그래밍 언

어용 도구와 함께 사전에 패키징되어 제공됩니다. 따라서 개발 머신을 위해 파일, SDK 및 플러그인을 설치하거나 구성할 필요 없이 몇 분 만에 인기 있는 애플리케이션 스택의 코드 작성을 시작할 수 있습니다. Cloud9은 클라우드 기반이므로, 손쉽게 여러 개의 개발 환경을 유지 관리하여 프로젝트 리소스를 격리할 수 있습니다.

## Cloud9 구성

AWS 관리 콘솔 - Cloud9 을 선택하고, Cloud9 서비스 화면으로 이동합니다.

Create environment 를 선택합니다.

New AWS Cloud9 environment

Create environment

**Step1.** Name environment에 아래와 같이 이름을 입력하고, Next step을 클릭합니다. 사용자의 Cloud9은 리전당 unique 해야 합니다. 각자 영문이름을 입력하세요.

mybuilders-xxxx

AWS Cloud9 > Environments > Create environment

Step 1  
Name environment

Step 2  
Configure settings

Step 3  
Review

### Name environment

**Environment name and description**

**Name**  
The name needs to be unique per user. You can update it at any time in your environment settings.

Limit: 60 characters

**Description - Optional**  
This will appear on your environment's card in your dashboard. You can update it at any time in your environment settings.

Limit: 200 characters

**Cancel** **Next step**

Step2. Configure settings 에서 기본값으로 사용하고, Cost-Saving setting - After four hours 를 선택합니다. 기본값은 30분이며, 30분 후에는 절전 모드로 변경됩니다. 랩에서는 4시간 동안 동작 시키도록 합니다.

The screenshot shows the 'Configure settings' step of the Cloud9 environment creation wizard. On the left, a sidebar lists 'Step 1 Name environment', 'Step 2 Configure settings' (which is active), and 'Step 3 Review'. The main area is titled 'Environment settings'.

**Environment type:** Info  
Run your environment in a new EC2 instance or an existing server. With EC2 instances, you can connect directly through Secure Shell (SSH) or connect via AWS Systems Manager (without opening inbound ports).

Create a new EC2 instance for environment (direct access)  
Launch a new instance in this region that your environment can access directly via SSH.

Create a new no-ingress EC2 instance for environment (access via Systems Manager)  
Launch a new instance in this region that your environment can access through Systems Manager.

Create and run in remote server (SSH connection)  
Configure the secure connection to the remote server for your environment.

**Instance type:**  
 t2.micro (1 GiB RAM + 1 vCPU)  
Free-tier eligible. Ideal for educational users and exploration.  
 t3.small (2 GiB RAM + 2 vCPU)  
Recommended for small-sized web projects.  
 m5.large (8 GiB RAM + 2 vCPU)  
Recommended for production and general-purpose development.  
 Other instance type  
Select an instance type.  
A dropdown menu shows 't3.nano'.

**Platform:**  
 Amazon Linux 2 (recommended)  
 Amazon Linux  
 Ubuntu Server 18.04 LTS

**Cost-saving setting:**  
Choose a predetermined amount of time to auto-hibernate your environment and prevent unnecessary charges. We recommend a hibernation settings of half an hour of no activity to maximize savings.  
A dropdown menu shows 'After four hours'.

**(i)** 여기서 잠깐!!!! Cloud9 인스턴스는 어디에 배치되나요?

기본 Default VPC의 Public Subnet에 배치 됩니다. 만약 다른 VPC를 사전에 구성해 두었다면 변경도 가능합니다.

Step3. Review 단계입니다. 앞서 생성한 내용을 검토하는 단계입니다.

Create environment 를 선택합니다.

Step 1  
**Name environment**

Step 2  
**Configure settings**

Step 3  
**Review**

## Review

### Environment name and settings

Name  
mybuilders

Description  
Cloud IDE for the AWS Builders Events

Environment type  
EC2

Instance type  
t2.micro

Subnet

Platform  
Amazon Linux 2 (recommended)

Cost-saving settings  
After four hours

IAM role  
AWSServiceRoleForAWSCloud9 (generated)

**We recommend the following best practices for using your AWS Cloud9 environment**

- Use **source control** and **backup** your environment frequently. AWS Cloud9 does not perform automatic backups.
- Perform regular **updates of software** on your environment. AWS Cloud9 does not perform automatic updates on your behalf.
- Turn on **AWS CloudTrail** in your AWS account to track activity in your environment. [Learn more](#)
- Only share your environment with **trusted users**. Sharing your environment may put your AWS access credentials at risk. [Learn more](#)

**Create environment**

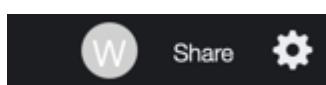
이제 2~3분 뒤면 EC2 인스턴스 기반의 Cloud IDE 생성됩니다.

## Cloud9 둘러보기 및 환경 구성

Cloud9은 훌륭한 Cloud IDE 환경을 제공합니다. Code 저작도구와 터미널 등을 제공하고 있기 때문에, 이 랩에서 활용해 볼니다.

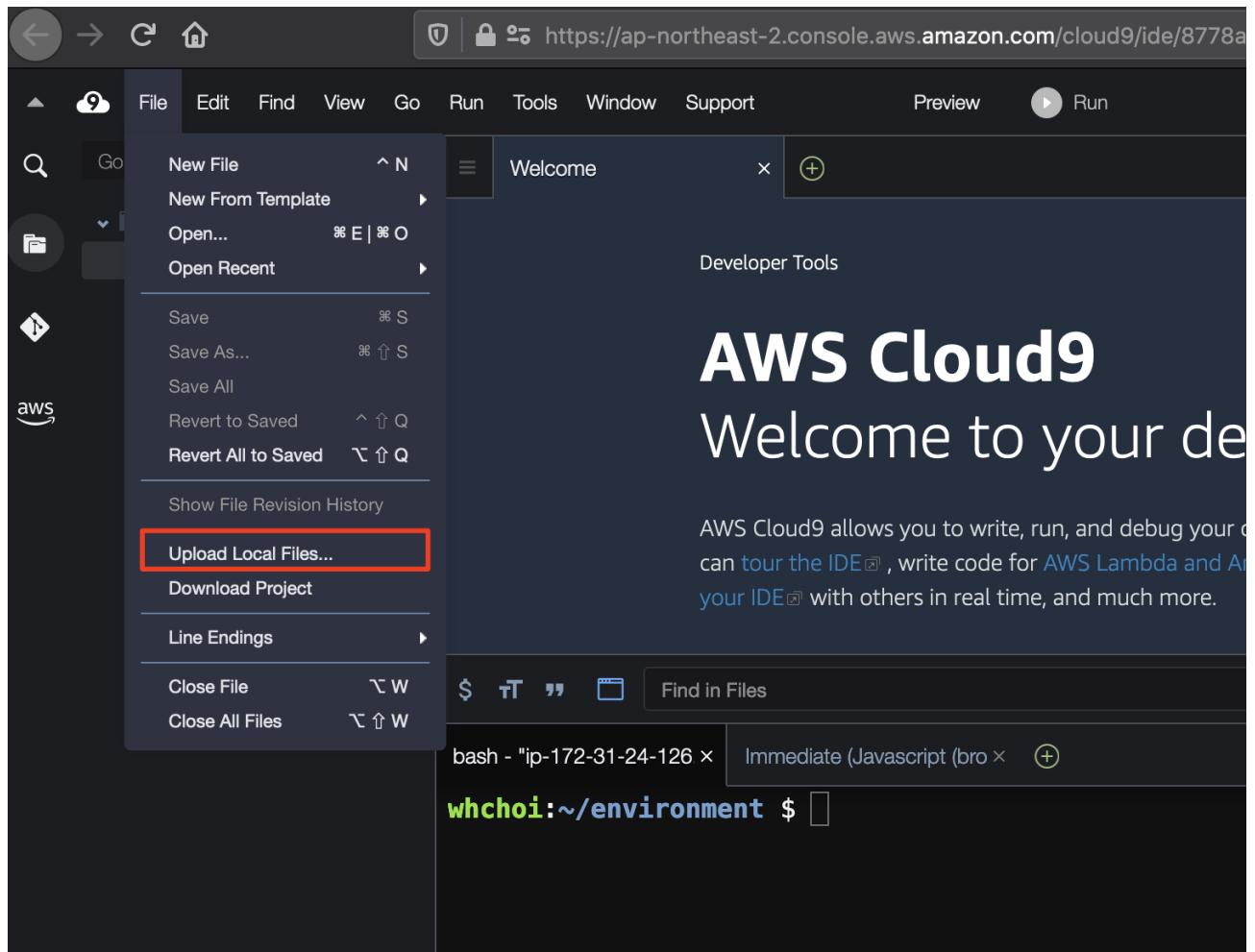
### 환경 설정

Cloud9 화면 우측 상단의 톱니바퀴 모양 Preference를 선택합니다.

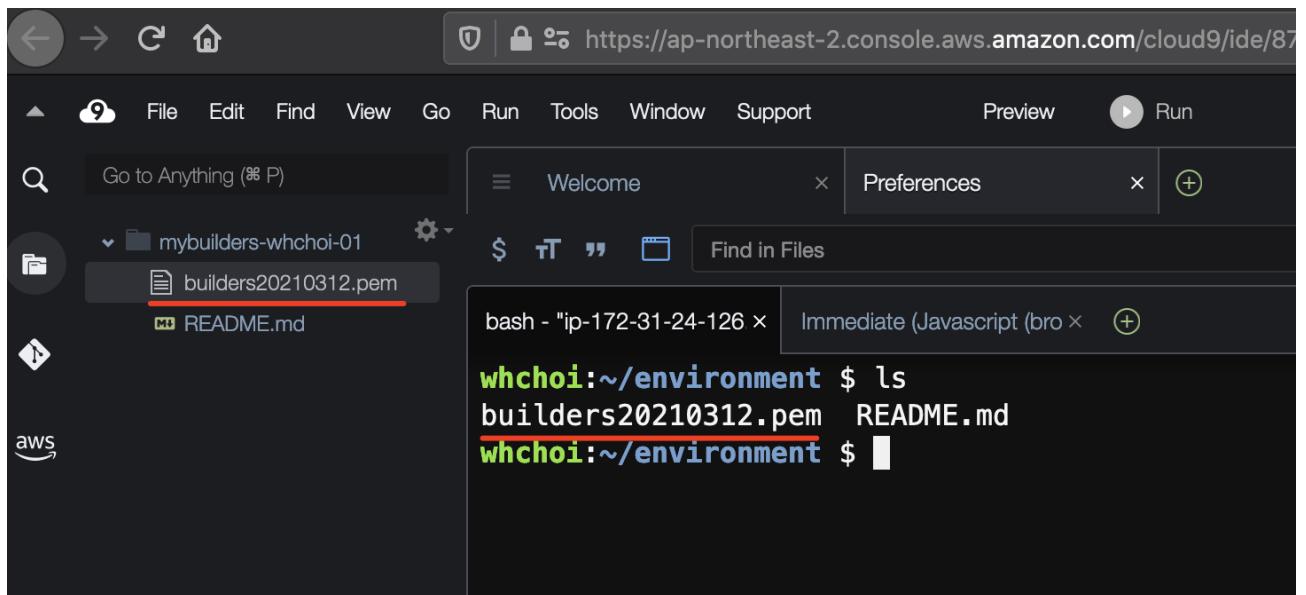


프로젝트, User 설정, 터미널 설 등 다양한 환경을 구성할 수 있습니다. (이 랩에서는 자세한 소개를 생략합니다.)

먼저 키 페어 만들기에서 생성하고, 로컬 PC로 다운로드 받은 pem key를 Cloud9 콘솔에 업로드 합니다.



정상적으로 업로드하였다면, 아래와 같이 확인 할 수 있습니다.

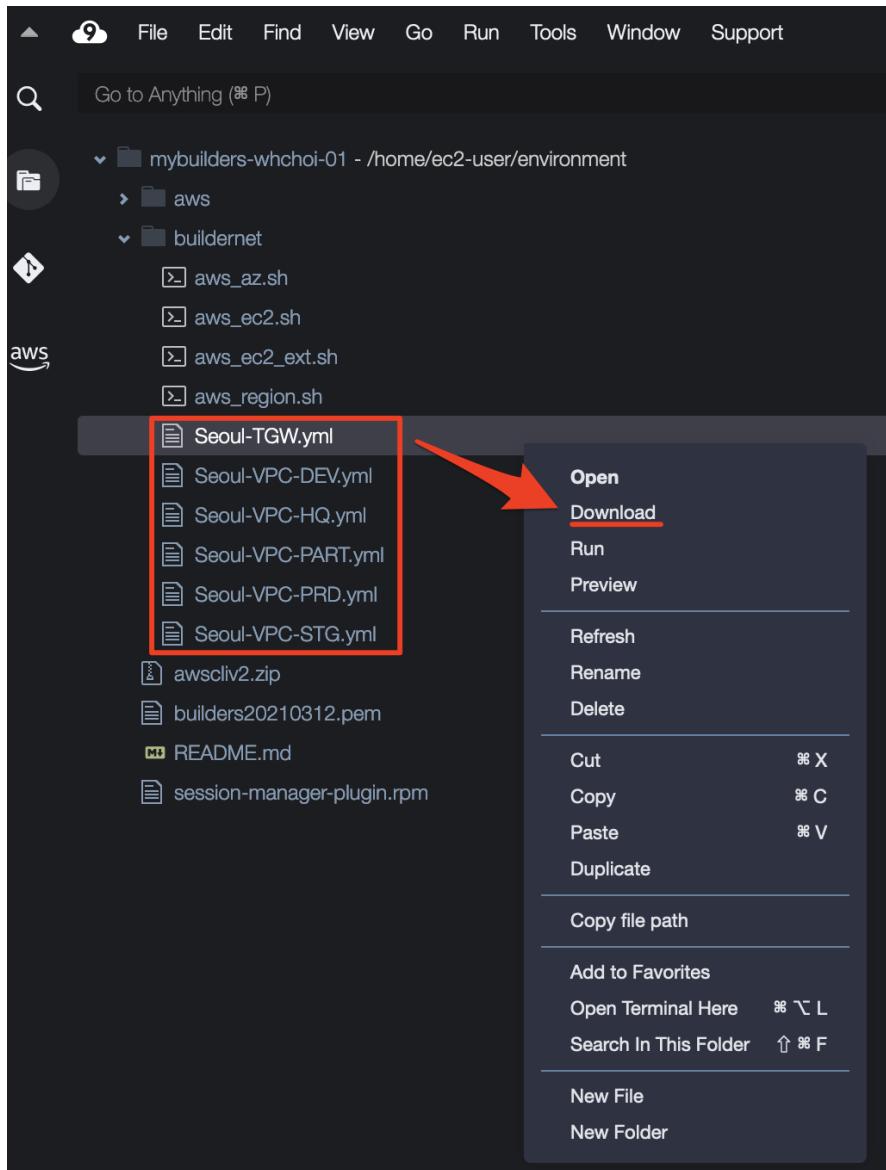


랩이 종료된 후에는 보안상 삭제합니다.

이 랩을 위해서 아래 내용을 복사해서 설치합니다.

```
1 ##aws cli version 2.0 upgrade
2 curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscli"
3 unzip awscliv2.zip
4 sudo ./aws/install
5
6 ##aws cli completer
7 which aws_completer
8 export PATH=/usr/local/bin:$PATH
9 source ~/.bash_profile
10 complete -C '/usr/local/bin/aws_completer' aws
11
12 ##aws ssm plugin install
13 curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux86_64/session-manager-plugin.rpm"
14 sudo yum install -y session-manager-plugin.rpm
15
16 ##source download
17 git clone https://github.com/whchoi98/buildernet.git
```

완료 된 이후 아래와 같이 Cloud9 좌측 패널에서 yml 파일을 다운로드 받습니다.



## 사전 준비 단계 과정

1. 키페어 만들기 - Private Key 와 Public Key 만들고, Private Key는 안전하게 로컬 PC에 내려 받습니다.
2. Cloud9 만들기 - Cloud9 을 생성합니다.
3. Cloud9 환경 구성 - 나만의 Cloud9 환경을 꾸미고, 이번 랩에서 필요한 설정들을 구성합니다.
  - PC에 내려받은 Private key를 복사해서, 동일한 이름으로 Cloud9에 업로드

- Cloud9 터미널에 aws cli v2 설치, aws cli 자동완성 설치
- Session manager plugin 설치
- LAB에서 사용될 Cloudformation용 YAML 파일과 Shell 다운로드

해당 LAB의 질문 사항은 [whchoi98@gmail.com](mailto:whchoi98@gmail.com)/ [whchoi@amazon.com](mailto:whchoi@amazon.com) 또는  [슬랙채널](#) (<https://whchoi-hol.slack.com/archives/C01QM79Q4BD>)에서 문의 가능합니다.

**TransitGateway**

# TransitGateway Overview

## 1. AWS Transit Gateway 소개

AWS Transit Gateway는 중앙 허브를 통해 VPC와 온프레미스 네트워크를 연결합니다. 복잡한 피어링 관계를 제거하여 네트워크를 간소화합니다. 클라우드 라우터 역할을 하므로 새로운 연결을 한 번만 추가하면 됩니다.

글로벌 확장 시 리전 간 피어링을 사용하면 [AWS 글로벌 네트워크](#)에서 AWS Transit Gateway를 하나로 연결할 수 있습니다.. 데이터는 자동으로 암호화되고 퍼블릭 인터넷을 통하지 않습니다. 중앙 위치에 있으므로 [AWS Transit Gateway 네트워크 관리자](#)를 사용하여 전체 네트워크를 보고 SD-WAN(소프트웨어 정의 광역 네트워크) 디바이스에 연결할 수 있습니다.

---

## 2. AWS Transit Gateway 사용 이점

### 간편한 연결

AWS Transit Gateway는 클라우드 라우터 역할을 하므로 네트워크 아키텍처가 간소화됩니다. 네트워크 확장 시 증가하는 연결 관리로 인한 복잡성이 발생하지 않습니다. 글로벌 애플리케이션을 구축하는 경우 리전 간 피어링을 사용하여 AWS Transit Gateway를 연결할 수 있습니다.

### 가시성 및 제어 향상

AWS Transit Gateway 네트워크 관리자를 사용하면 중앙 콘솔에서 Amazon VPC 및 엣지 연결을 손쉽게 모니터링할 수 있습니다. 주요 SD-WAN 디바이스와 통합되므로 AWS Transit Gateway 네트워크 관리자를 사용하여 문제를 빠르게 식별하고 글로벌 네트워크의 이벤트에 대응할 수 있습니다.

### 향상된 보안

Amazon VPC와 AWS Transit Gateway 간의 트래픽은 AWS의 글로벌 프라이빗 네트워크에서 유지되며 퍼블릭 인터넷에 노출되지 않습니다. AWS Transit Gateway 리전 간 피어링은 단일

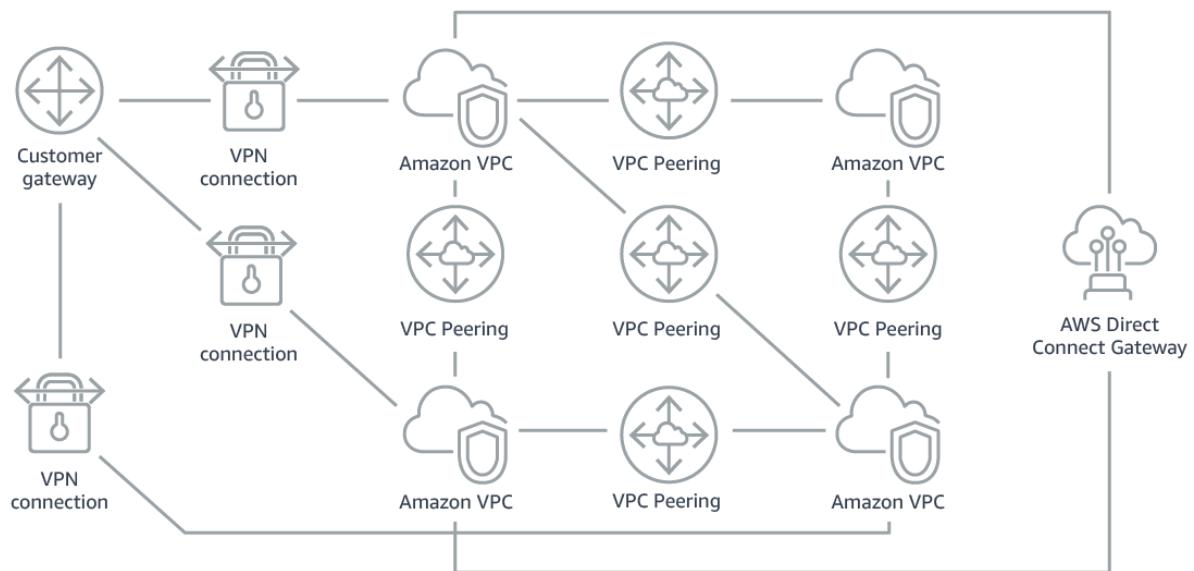
장애 발생 지점이나 대역폭 병목 없이 모든 트래픽을 암호화합니다. 따라서 DDoS(분산 서비스 거부) 공격 및 기타 일반적인 익스플로잇을 차단하는 데 도움이 됩니다.

## 유연한 멀티캐스트

AWS Transit Gateway 멀티캐스트 지원은 동일한 콘텐츠를 다수의 특정 대상으로 분산합니다. 광범위한 온프레미스 멀티캐스트 네트워크가 필요하지 않으며 화상 회의, 미디어 또는 전화 회의와 같은 처리량이 많은 애플리케이션에 필요한 대역폭이 감소합니다.

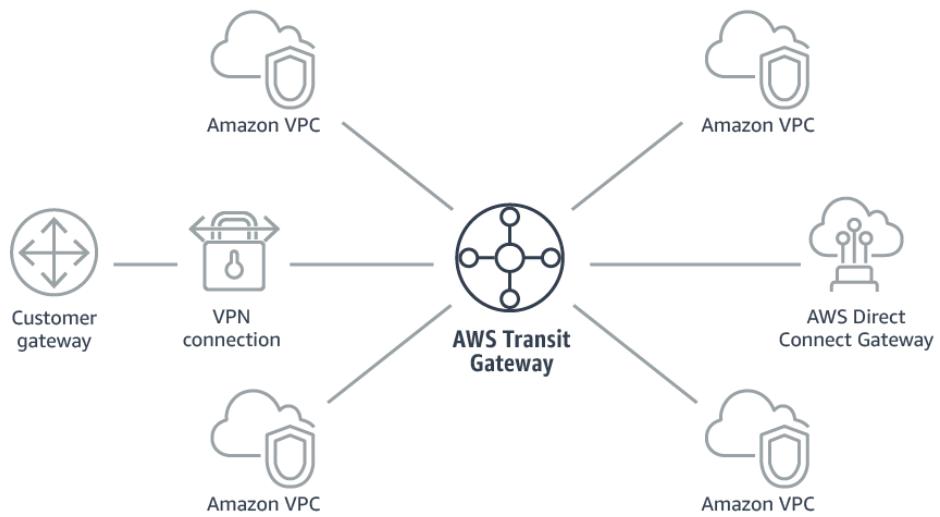
## 3. 네트워크 간소화 디자인

### AWS Transit Gateway 미사용 시



확장할 때마다 복잡성이 증가합니다. 각 VPC 안에 라우팅 테이블을 유지해야 하고 개별 네트워크 게이트웨이를 사용하여 각 온사이트 위치에 연결해야 합니다.

### AWS Transit Gateway 사용 시



네트워크가 간소화되고 확장성이 개선됩니다. AWS Transit Gateway가 각 VPC 또는 VPN 간의 모든 트래픽을 라우팅하므로, 단일 위치에서 모든 트래픽을 관리하고 모니터링할 수 있습니다.

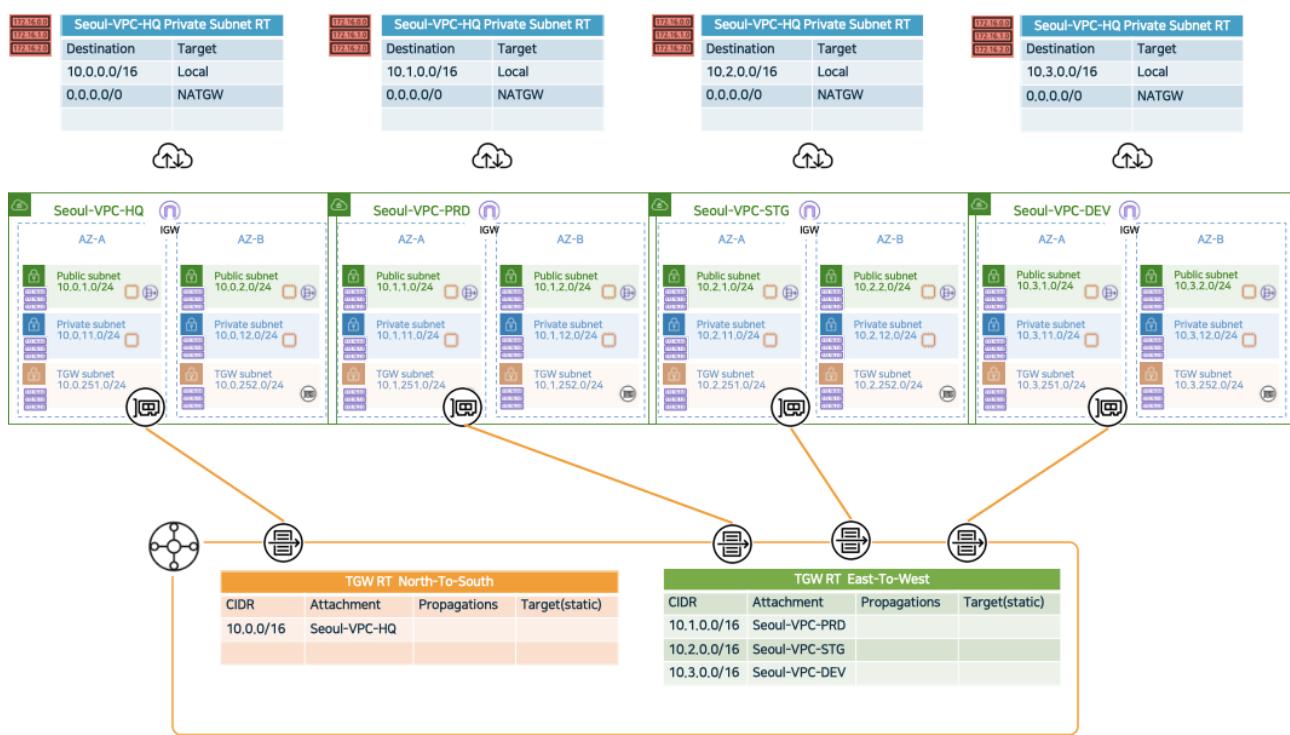
# TransitGateway 구성하기

## 1. TransitGateway 기본 구성

### 구성 아키텍쳐 소개

AWS TransitGateway의 기본 동작 이해를 위해, 가장 기본이 되는 디자인을 먼저 구성해 볼니다.

아래 그림은 이번 Chapter에서 구성해 볼 아키텍쳐입니다.



### Task1. VPC 구성하기

Cloudformation을 통해 기본이 되는 VPC구성을 먼저 구성합니다.

#### 1. 사전 준비하기

서울 리전에 4개의 VPC를 구성하고, 사전에 구성된 TGW를 배포합니다.

아래 Github에서 실습에 사용할 Cloudformation yaml 파일을 다운로드 받습니다.

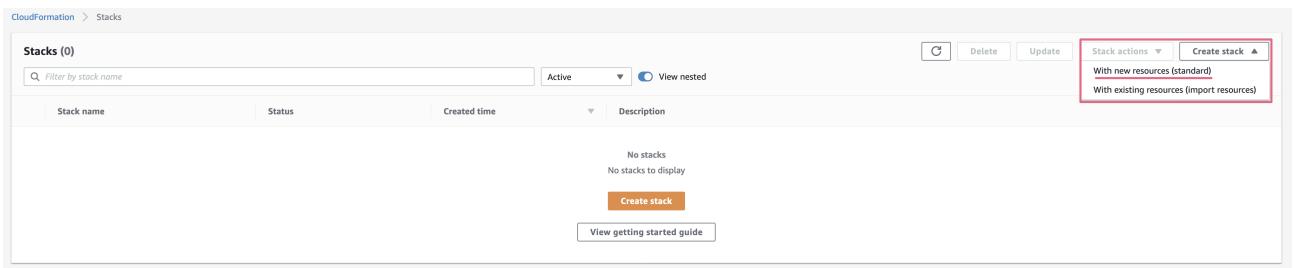
```
git clone https://github.com/whchoi98/builders20210312
```

## 2. Cloudformation 생성.

Seoul-VPC-HQ, Seoul-VPC-PRD, Seoul-VPC-STG, Seoul-VPC-DEV를 Cloudformation 을 기반으로 생성합니다.

AWS 콘솔에서 서울 리전 (ap-northeast-2)를 선택하고, Cloudformation 서비스를 선택합니다.

Cloudformation에서 먼저 새로운 스택을 생성합니다.



앞서 다운로드 받은 yaml 파일들 중에 `Seoul-VPC-HQ.yaml` 파일을 업로드 합니다.

Seoul-VPC-HQ

1단계  
템플릿 지정2단계  
스택 세부 정보 지정3단계  
스택 옵션 구성4단계  
검토

## 스택 생성

### 사전 조건 - 템플릿 준비

템플릿 준비 모든 스택은 템플릿을 기반으로 합니다. 템플릿은 JSON 또는 YAML 텍스트 파일로, 스택에 포함하려는 AWS 리소스에 대한 구성 정보가 들어 있습니다.

 준비된 템플릿 샘플 템플릿 사용 Designer에서 템플릿 생성

### 템플릿 지정

템플릿은 스택의 리소스와 속성을 설명하는 JSON 또는 YAML 파일입니다.

#### 템플릿 소스

템플릿을 선택하면 템플릿이 저장될 Amazon S3 URL이 생성됩니다.

 Amazon S3 URL 템플릿 파일 업로드

#### 템플릿 파일 업로드

 파일 선택

Seoul-VPC-HQ.yaml

JSON 또는 YAML 형식 파일

S3 URL: <https://s3.ap-northeast-2.amazonaws.com/cf-templates-12p302ou0syqq-ap-northeast-2/20210681Kp-Seoul-VPC-HQ.yaml>[Designer에서 보기](#)

취소

다음

다음을 선택하고, 아래와 같아 스택이름은 파일명과 동일하게 입력합니다.

### 스택 세부 정보 지정

#### 스택 이름

스택 이름

Seoul-VPC-HQ

파일명과 동일하게 입력합니다.

스택 이름은 문자(A-Z 및 a-z), 숫자(0-9) 및 대시(-)를 포함할 수 있습니다.

**!** 스택이름을 파일명과 다르게 입력하지 마십시오. 이후 과정에서 TransitGateway의 yaml파일은 , VPC yml 에서 생성된 값들을 import 해서 TGW를 생성합니다. 스택이름을 파일명과 다르게 할 경우, TGW를 생성할 때 에러가 발생합니다.

별도로 설정 변경없이, 다음 단계를 진행하고, 승인을 선택하고 스택생성합니다.

▶ 빠른 생성 링크

기능

**! The following resource(s) require capabilities: [AWS::IAM::InstanceProfile, AWS::IAM::Role]**이 템플릿에는 자격 증명 및 액세스 관리(IAM) 리소스가 들어 있습니다. 각 리소스를 생성할 것인지 그리고 그러한 리소스가 필요한 최소 권한을 가지고 있는지 확인합니다. 또한 이러한 리소스는 사용자 지정 이름을 가집니다. 사용자 지정 이름이 해당 AWS 계정에서 고유한지 확인합니다. [자세히 알아보기](#) AWS CloudFormation에서 사용자 지정 이름으로 IAM 리소스를 생성할 수 있음을 승인합니다.

취소

이전

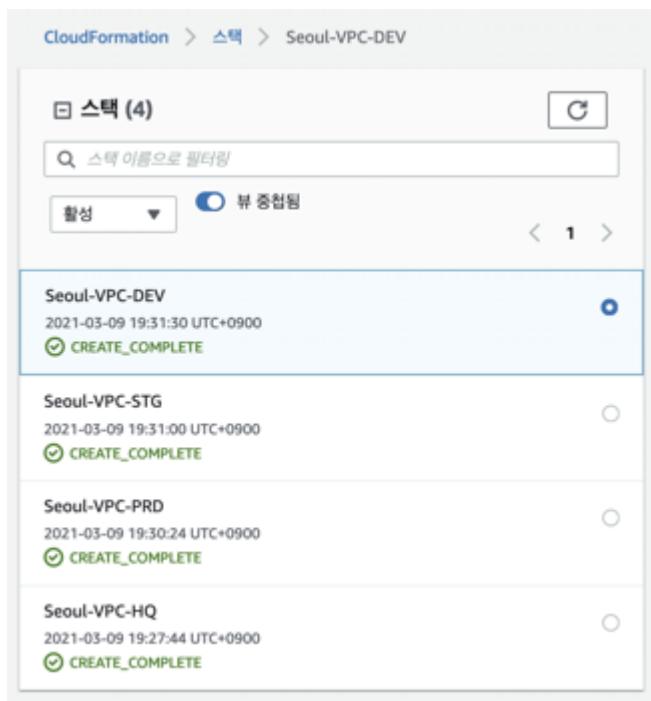
변경 세트 만들기

스택 생성

다운로드 받은 yaml 파일 3개를 추가로 반복적으로 수행합니다.

- 1 Seoul-VPC-PRD
- 2 Seoul-VPC-STG
- 3 Seoul-VPC-DEV

4개의 VPC가 모두 정상적으로 구성되면 아래와 같이 Cloudformation에서 확인 할 수 있습니다. 4개의 VPC는 각 3분 내외에 생성됩니다. 동시에 수행해도 가능합니다.



## Task2. TGW구성하기.

4개의 VPC를 연결할 TransitGateway를 Region에 Cloudformation으로 생성합니다.

## 스택 생성

### 사전 조건 - 템플릿 준비

#### 템플릿 준비

모든 스택은 템플릿을 기반으로 합니다. 템플릿은 JSON 또는 YAML 텍스트 파일로, 스택에 포함하려는 AWS 리소스에 대한 구성 정보가 들어 있습니다.

준비된 템플릿

샘플 템플릿 사용

Designer에서 템플릿 생성

### 템플릿 지정

템플릿은 스택의 리소스와 속성을 설명하는 JSON 또는 YAML 파일입니다.

#### 템플릿 소스

템플릿을 선택하면 템플릿이 저장될 Amazon S3 URL이 생성됩니다.

Amazon S3 URL

템플릿 파일 업로드

#### 템플릿 파일 업로드

파일 선택  Seoul-TGW.yml

JSON 또는 YAML 형식 파일

S3 URL: <https://s3.ap-northeast-2.amazonaws.com/cf-templates-12p302ou0sygq-ap-northeast-2/20210688Sg-Seoul-TGW.yml>

[Designer에서 보기](#)

취소

**다음**

다음을 선택하고, 아래와 같아 스택 이름은 파일명과 동일하게 입력합니다. (TGW는 스택 이름을 다르게 지정해도, 본 랙을 구성하는데 문제가 없습니다.)

## 스택 세부 정보 지정

### 스택 이름

#### 스택 이름

Seoul-TGW

**Stack 이름을 파일명과 동일하게 입력합니다.**

스택 이름은 문자(A-Z 및 a-z), 숫자(0-9) 및 대시(-)를 포함할 수 있습니다.

5분 이내에 TransitGateway가 완성됩니다.

CloudFormation > 스택 > Seoul-TGW

스택 (5)

Seoul-TGW  
2021-03-09 19:41:16 UTC+0900  
CREATE\_COMPLETE

Seoul-VPC-DEV  
2021-03-09 19:31:30 UTC+0900  
CREATE\_COMPLETE

Seoul-VPC-STG  
2021-03-09 19:31:00 UTC+0900  
CREATE\_COMPLETE

Seoul-VPC-PRD  
2021-03-09 19:30:24 UTC+0900  
CREATE\_COMPLETE

Seoul-VPC-HQ  
2021-03-09 19:27:44 UTC+0900  
CREATE\_COMPLETE

## 2. TransitGateway 구성 확인

### Task3. VPC, EC2 구성 확인

AWS 관리콘솔 - VPC를 선택합니다.

4개의 VPC가 정상적으로 생성되었는지 확인합니다.

VPC (5) 정보											작업	VPC 생성
	Name	VPC ID	상태	IPv4 CIDR	DHCP 옵션 세트	기본 라우팅 테이블	기본 네트워크 ACL	테넌시	기본 VPC			
<input type="checkbox"/>	Default-VPC	vpc-e02e858b	Available	172.31.0.0/16	dopt-da920db1	rtb-b15727da	acl-e24bf89	Default	예			
<input type="checkbox"/>	Seoul-VPC-DEV	vpc-0e45aab6bdeec03	Available	10.3.0.0/16	dopt-da920db1	rtb-082dcf4bbbc52bab	acl-031e98c43132b5163	Default	아니요			
<input type="checkbox"/>	Seoul-VPC-HQ	vpc-0f998522f59c79768	Available	10.0.0.0/16	dopt-da920db1	rtb-09afead91e9fe6ee	acl-0b4ac9a241cb9db66	Default	아니요			
<input type="checkbox"/>	Seoul-VPC-PRD	vpc-0fb93a230e2505bfc	Available	10.1.0.0/16	dopt-da920db1	rtb-07b70c4ad83eac800	acl-0392defd63e73c428	Default	아니요			
<input type="checkbox"/>	Seoul-VPC-STG	vpc-05e0d6104d2a57256	Available	10.2.0.0/16	dopt-da920db1	rtb-0d5f22d4e9f8ca492	acl-0b7047dc92668f97b	Default	아니요			

AWS 관리콘솔 - EC2를 선택합니다.

EC2가 정상적으로 생성되었는지 확인합니다.

인스턴스 (32) 정보										
인스턴스 필터링		인스턴스 상태: running								
인스턴스 상태: running		필터 지우기								
Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	기용 영역	피블릭 IPv4 DNS	피블릭 IPv4 주소	단락주	
Seoul-VPC-DEV-Private-10.3.22.101	i-06e77dc893d5069b2	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	-	-	
Seoul-VPC-STG-Private-10.2.22.101	i-08194459730612d10	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	-	-	
Seoul-VPC-HQ-Public-10.0.12.102	i-0aa1c4c96fb924b33	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	ec2-3-34-195-174.ap.nor... 3.34.195.174	-	
Seoul-VPC-DEV-Public-10.3.12.101	i-0a2bddf757fc89d73	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	ec2-3-3g-14-239.ap.northe... 3.36.14.239	-	
Seoul-VPC-DEV-Private-10.3.22.102	i-0db8bede61e8ca32f2	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	-	-	
Seoul-VPC-STG-Public-10.2.12.102	i-0479efabde92336f1	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	ec2-3-3g-13-174.ap.northe... 3.36.13.174	-	
Seoul-VPC-PRD-Public-10.1.12.101	i-01ff71a781ce44ff	● 실행 중	t3.small	● 2/2개 검사 통과	경보 있음	+	ap-northeast-2b	ec2-15-164-236-227.ap.nor... 15.164.236.227	-	
Seoul-VPC-DEV-Public-10.3.12.102	i-07e5f3b23f1ea3ad7	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	ec2-15-165-228-28.ap.nort... 15.165.228.28	-	
Seoul-VPC-STG-Private-10.2.22.102	i-00a39b2a7f1759f90	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	-	-	
Seoul-VPC-HQ-Private-10.0.22.101	i-078a899d467028886	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	-	-	
Seoul-VPC-HQ-Private-10.0.22.102	i-0a7398a27fe7d07f4	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	-	-	
Seoul-VPC-PRD-Private-10.1.22.101	i-02dd4d59310945eba4	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	-	-	
Seoul-VPC-STG-Public-10.2.12.101	i-0dc3f34c94c7bf323	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	ec2-15-165-231-145.ap.nor... 15.165.231.145	-	
Seoul-VPC-PRD-Private-10.1.22.102	i-0e25256ac520cdde4	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	-	-	
Seoul-VPC-PRD-Public-10.1.12.102	i-0ea45cf007de0dab3	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	ec2-15-164-178-209.ap.nor... 15.164.178.209	-	
Seoul-VPC-HQ-Public-10.0.12.101	i-02717f5415d127e0	● 실행 중	t3.small	● 2/2개 검사 통과	경보 없음	+	ap-northeast-2b	ec2-15-164-173-76.ap.nort... 15.164.173.76	-	
Seoul-VPC-PRD-Private-10.0.21.101	i-0a8ea21a26a5770a	● 실행 중	t2.small	● 7/7개 검사 통과	경보 없음	+	ap-northeast-2b	-	-	

## Task 4. TGW 구성 확인

VPC - TransitGateway를 선택해서, Transit Gateway 정상적으로 구성되었는지 확인합니다.

### ▼ TRANSIT GATEWAY

#### Transit Gateway

##### Transit Gateway 연결

##### Transit Gateway 라우팅 테이블

##### Transit Gateway 멀티캐스트

##### 네트워크 관리자

State : available																												
Name	Transit Gateway ID	Owner ID	State																									
Seoul-TGW	tgw-0408d8883c27453ea	606879168280	available																									
	tgw-0427a45e96fc9bff2	606879168280	available																									
<b>Transit Gateway:</b> tgw-0408d8883c27453ea																												
<a href="#">Details</a> <a href="#">Tags</a> <a href="#">Sharing</a>																												
<table> <tbody> <tr> <td>Transit Gateway ID</td><td>tgw-0408d8883c27453ea</td> <td>Owner account ID</td><td>606879168280</td> </tr> <tr> <td>State</td><td>available</td> <td>Amazon ASN</td><td>65001</td> </tr> <tr> <td>DNS support</td><td>enable</td> <td>VPN ECMP support</td><td>enable</td> </tr> <tr> <td>Auto accept shared attachments</td><td>enable</td> <td>Default association route table</td><td>disable</td> </tr> <tr> <td>Association route table ID</td><td>-</td> <td>Default propagation route table</td><td>disable</td> </tr> <tr> <td>Propagation route table ID</td><td>-</td> <td>Multicast support</td><td>disable</td> </tr> </tbody> </table>					Transit Gateway ID	tgw-0408d8883c27453ea	Owner account ID	606879168280	State	available	Amazon ASN	65001	DNS support	enable	VPN ECMP support	enable	Auto accept shared attachments	enable	Default association route table	disable	Association route table ID	-	Default propagation route table	disable	Propagation route table ID	-	Multicast support	disable
Transit Gateway ID	tgw-0408d8883c27453ea	Owner account ID	606879168280																									
State	available	Amazon ASN	65001																									
DNS support	enable	VPN ECMP support	enable																									
Auto accept shared attachments	enable	Default association route table	disable																									
Association route table ID	-	Default propagation route table	disable																									
Propagation route table ID	-	Multicast support	disable																									

## Task5. TGW Attachment 확인.

VPC-Transit Gateway-Transit Gateway 연결 을 선택해서, Transit Gateway attachment가 정상적으로 구성되었는지 확인합니다.

Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State	Associated route table ID	Association state
Seoul-TGW-Attach-Seoul-VPC-STG	tgw-attach-0e3367ffc77a56807	tgw-0408d8883c27453...	VPC	vpc-05e0d6104d2a57256	available	tgw-rtb-0e0cb51fd169e86f	associated
Seoul-TGW-Attach-Seoul-VPC-PRD	tgw-attach-03b55a9871718d37c	tgw-0408d8883c27453...	VPC	vpc-0fb93a230e2505bfc	available	tgw-rtb-0e0cb51fd169e86f	associated
<b>Seoul-TGW-Attach-Seoul-VPC-HQ</b>	<b>tgw-attach-085547c8aa4620ef8</b>	<b>tgw-0408d8883c27453...</b>	VPC	<b>vpc-0f998522f59c79768</b>	available	<b>tgw-rtb-0006f933726970080</b>	<b>associated</b>
Seoul-TGW-Attach-Seoul-VPC-DEV	tgw-attach-0405e1b969c803e9e	tgw-0408d8883c27453...	VPC	vpc-0e45aab6bdeedec03	available	tgw-rtb-0e0cb51fd169e86f	associated
	tgw-attach-0a8b020c1f2f92232	tgw-0427a45e9fc9bf2	VPC	vpc-0c9faf037e982cb38	available	-	-

Seoul-TGW-Attach-Seoul-VPC-HQ를 선택하면, 이미 "Seoul-VPC-HQ"의 TGW-Subnet ID에 연결되어 있는 것을 확인할 수 있습니다. 또한 Routing Table에 Association 된 상태도 확인이 가능합니다.

1. TGW Routing Table과 Attachment가 연결된 상태를 확인
2. Attachment가 VPC의 어떤 Subnet과 연결되었는지 확인

Details	Tags
<p>Transit Gateway attachment ID tgw-attach-085547c8aa4620ef8 Transit Gateway ID tgw-0408d8883c27453ea Resource type VPC Resource ID vpc-0f998522f59c79768 <b>1 Association state associated</b> IPv6 support disable</p>	<p>Transit Gateway owner ID 606879168280 Resource owner account ID 606879168280 State available <b>1 Associated route table tgw-rtb-0006f933726970080</b> <b>2 Subnet IDs subnet-0b2c0d46ecccfc227 subnet-0e5e4d50c922da596</b></p>

아래에서 나머지 VPC들도 선택해서 확인해 봅니다.

- 1 Seoul-TGW-Attach-Seoul-VPC-STG
- 2 Seoul-TGW-Attach-Seoul-VPC-DEV
- 3 Seoul-TGW-Attach-Seoul-VPC-PRD

## Task6. TGW Routing Table 확인.

VPC-Transit Gateway-Transit Gateway- Transit Gateway 라우팅 테이블 을 선택해서 라우팅 테이블 구성은 확인해 봅니다. 라우팅 테이블은 2개로 구성되어 있습니다.

East-To-West 트래픽을 위한 라우팅 테이블 도메인, North-To-South 트래픽을 위한 라우팅 테이블 도메인으로 구성되어 있습니다. Seoul-VPC-HQ 는 North-To-South 라우팅 테이블 도메인에 속해 있습니다.

먼저 North-To-South 라우팅 테이블 도메인을 확인합니다.

해당 라우팅 테이블 도메인에는 Seoul-VPC-HQ를 연결했습니다.

Associations와 Propagation 탭을 눌러서, Seoul-VPC-HQ 연결과 Seoul-VPC-HQ의 CIDR가 정상적으로 업데이트 되었는지 확인합니다.

Details	Associations	Propagations	Prefix list references	Routes	Tags
<a href="#">Create association</a> <a href="#">Delete association</a>					
속성별 필터 또는 키워드별 검색					
Attachment ID	Resource type	Resource ID	State		
tgw-attach-085547c8aa4620ef8	VPC	vpc-0f998522f59c79768	associated		

Details	Associations	Propagations	Prefix list references	Routes	Tags
<a href="#">Create propagation</a> <a href="#">Delete propagation</a>					
속성별 필터 또는 키워드별 검색					
Attachment ID	Resource type	Resource ID	State		
tgw-attach-085547c8aa4620ef8	VPC	vpc-0f998522f59c79768	enabled		

propagation이 정상적으로 구성되었기 때문에 Route 탭을 선택하면, Route Type은 Propagated 되었다고 표기됩니다.

Details	Associations	Propagations	Prefix list references	Routes	Tags
The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.					
<a href="#">Create static route</a> <a href="#">Replace static route</a> <a href="#">Delete static route</a>					
속성별 필터 또는 키워드별 검색					
CIDR	Attachment	Resource type	Route type	Route state	
10.0.0.0/16	tgw-attach-085547c8aa4620ef8   vpc-0f998522f59c79768	VPC	propagated	active	

이제 East-To-West 라우팅 테이블 도메인을 확인합니다.

해당 라우팅 테이블 도메인에는 Seoul-VPC-PRD, Seoul-VPC-STG, Seoul-VPC-DEV를 연결했습니다.

Transit Gateway route table						
Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table	Action
Seoul-TGW-RT-North-To-South	tgw-rtb-0006f933726970080	tgw-0408d8883c27453ea	available	No	No	
<input checked="" type="checkbox"/> Seoul-TGW-RT-East-To-West	tgw-rtb-0e0cb51fd169e86f	tgw-0408d8883c27453ea	available	No	No	
	tgw-rtb-00580867329736172	tgw-0427a45e96fc9bfff2	available	Yes	Yes	

East-To-West Routing Table 도메인을 선택하여, 라우팅 테이블 속성을 확인합니다.

Association 탭을 선택해서 3개의 VPC가 Association 되었는지 확인합니다.

Association							
Create association		Delete association					
Attachment							
Attachment							
Attachment ID	Resource type	Resource ID	State				
<input type="checkbox"/> tgw-attach-0e3367ffc77a56807	VPC	vpc-05e0d6104d2a57256	associated				
<input type="checkbox"/> tgw-attach-0405e1b969c803e9e	VPC	vpc-0e45aab6bdedeeec03	associated				
<input type="checkbox"/> tgw-attach-03b55a9871718d37c	VPC	vpc-0fb93a230e2505bfc	associated				

Propagations 탭을 선택해서, 3개의 VPC CIDR를 Propagation 하는지 확인합니다.

Propagation							
Create propagation		Delete propagation					
Attachment							
Attachment							
Attachment ID	Resource type	Resource ID	State				
<input type="checkbox"/> tgw-attach-03b55a9871718d37c	VPC	vpc-0fb93a230e2505bfc	enabled				
<input type="checkbox"/> tgw-attach-0405e1b969c803e9e	VPC	vpc-0e45aab6bdedeeec03	enabled				
<input type="checkbox"/> tgw-attach-0e3367ffc77a56807	VPC	vpc-05e0d6104d2a57256	enabled				

Routing 탭을 선택해서, 앞서 Propagation 된 Route가 정상적으로 등록되었는지 확인합니다.

	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.1.0.0/16	tgw-attach-03b55a9871718d37c   vpc-0fb93a230e2505bfc	VPC	propagated	active
<input type="checkbox"/>	10.2.0.0/16	tgw-attach-0e3367ffc77a56807   vpc-05e0d6104d2a57256	VPC	propagated	active
<input type="checkbox"/>	10.3.0.0/16	tgw-attach-0405e1b969c803e9e   vpc-0e45aab6bdedee03	VPC	propagated	active

**Cloudformation을 통해서 모두 정상적으로 구성되었습니다.**

해당 라우팅테이블 도메인에는 Seoul-VPC-PRD, Seoul-VPC-STG, Seoul-VPC-DEV만 연결되어 있습니다.

### 3. TGW 기반 트래픽 제어

#### Task7. SSM에서 인스턴스 확인

모든 랩의 구성 시험은 Private 인스턴스로 시험합니다. Cloudformation을 통해 System Manager와 Session Manager를 사용할 수 있도록 자동 배포 구성하였습니다.

Session Manager를 사용할 수 있도록 아래 같이 각 PC환경에 맞추어서 AWS Session Manager Plugin을 설치합니다. Cloud9을 사용하거나 웹콘솔에서 Session Manager를 사용하면 각 PC환경에서 설치할 필요가 없습니다.

- (i) PC 환경에서는 사전에 반드시 AWS CLI를 설치합니다. Cloud9으로 사용할 때는 별도 구성하지 않아도 됩니다.

#### Windows Session manager plugin 설치 (Cloud9, 웹기반 세션 매니저 사용시 생략)

```
https://s3.amazonaws.com/session-manager-downloads/plugin/latest/windows/Ses
```

## Mac OS용 Session manager plugin 설치(Cloud9, 웹기반 세션 매니저 사용시 생략)

번들 설치 관리자를 다운로드합니다.

```
curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/mac/s
```

패키지의 압축을 풁니다.

```
unzip sessionmanager-bundle.zip
```

설치 명령을 실행합니다.

```
sudo ./sessionmanager-bundle/install -i /usr/local/sessionmanagerplugin -b /
```

## Fedora Linux에서 Session Manager Plugin 설치(Cloud9, 웹기반 세션 매니저 사용시 생략)

```
1 curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux/sessionmanagerplugin.rpm"
2 sudo yum install -y session-manager-plugin.rpm
```

## Ubuntu에서 Session Manager Plugin 설치(Cloud9, 웹기반 세션 매니저 사용시 생략)

```
1 curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu/sessionmanagerplugin.deb"
2 sudo dpkg -i session-manager-plugin.deb
```

아래와 같이 Cloud9에서 shell을 실행해 봅니다.

```
1 ~/environment/buildernet/aws_ec2_ext.sh |grep "Seoul-VPC-HQ"
```

```
2 ~/environment/buildernet/aws_ec2_ext.sh |grep "Seoul-VPC-PRD"
3 ~/environment/buildernet/aws_ec2_ext.sh |grep "Seoul-VPC-STG"
4 ~/environment/buildernet/aws_ec2_ext.sh |grep "Seoul-VPC-DEV"
5
```

실행한 예제입니다.

```
1 ~/environment/buildernet/aws_ec2_ext.sh | grep "Seoul-VPC-HQ"
2 | Seoul-VPC-HQ-Public-10.0.12.102 | ap-northeast-2b | i-0aa1c4c96f8924
3 | Seoul-VPC-HQ-Private-10.0.22.101 | ap-northeast-2b | i-078a899d467028
4 | Seoul-VPC-HQ-Private-10.0.22.102 | ap-northeast-2b | i-0a7398a27be7d0
5 | Seoul-VPC-HQ-Public-10.0.12.101 | ap-northeast-2b | i-02717f54153d12
6 | Seoul-VPC-HQ-Private-10.0.21.101 | ap-northeast-2a | i-0c46e31a566a57
7 | Seoul-VPC-HQ-Public-10.0.11.101 | ap-northeast-2a | i-03a97a2e31d509
8 | Seoul-VPC-HQ-Public-10.0.11.102 | ap-northeast-2a | i-060471cb2d8294
9 | Seoul-VPC-HQ-Private-10.0.21.102 | ap-northeast-2a | i-0f36233e7389fe
10
```

ssm plugin을 통해서 인스턴스 ID 기반으로, 직접 Private Instance에 접속합니다. 인스턴스 ID는 **"aws\_ec2.sh"** 을 통해 확인 할 수 있습니다.

아래와 같은 명령을 통해서 직접 4개의 Private Instance에 접속합니다. (10.0.21.101, 10.1.21.101, 10.2.21.101, 10.2.31.101)

- **Seoul-VPC-HQ-Private-10.0.21.101**
- **Seoul-VPC-PRD-Private-10.1.21.101**
- **Seoul-VPC-STG-Private-10.2.21.101**
- **Seoul-VPC-DEV-Private-10.3.21.101**

```
aws ssm start-session --target "인스턴스 ID"
```

Cloud9에서 터미널 창을 4개를 추가로 오픈하고, 아래와 같이 각 4개의 호스트에 명령을 입력하여, bash 콘솔로 접속하고, 시험할 호스트들을 host file에 등록합니다.

- **Seoul-VPC-HQ-Private-10.0.21.101**

- Seoul-VPC-PRD-Private-10.1.21.101
- Seoul-VPC-STG-Private-10.2.21.101
- Seoul-VPC-DEV-Private-10.3.21.101

```
1 sudo -s
2 echo 10.0.21.101 SEOUL-VPC-HQ-Private >> /etc/hosts
3 echo 10.1.21.101 SEOUL-VPC-PRD-Private >> /etc/hosts
4 echo 10.2.21.101 SEOUL-VPC-STG-Private >> /etc/hosts
5 echo 10.3.21.101 SEOUL-VPC-DEV-Private >> /etc/hosts
6 echo 10.4.21.101 SEOUL-VPC-PRT-Private >> /etc/hosts
7 echo 10.5.21.101 IAD-VPC-Private >> /etc/hosts
8
```

## Task8. 시나리오 이해하기

다음과 같은 시나리오 구성으로 Task9~11를 수행합니다.

1. 빌더스 컴퍼니는 아래와 같은 VPC를 하나의 계정에 소유하고 있습니다.

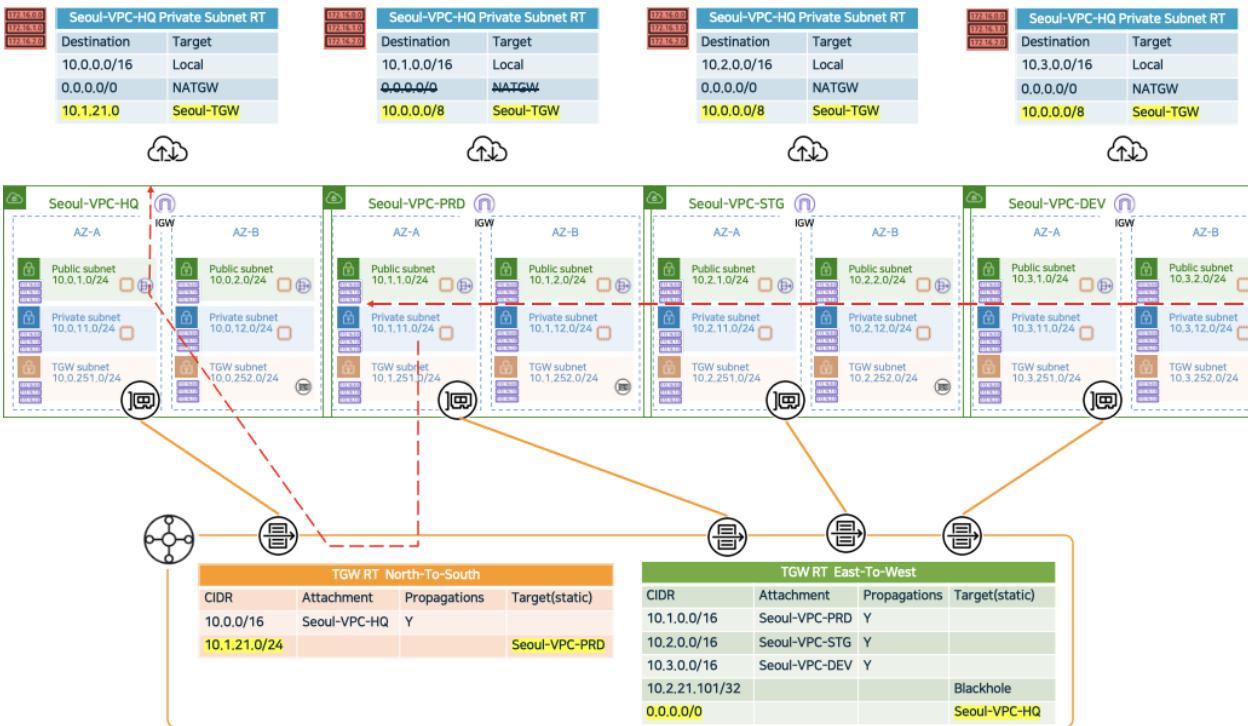
- IT Control Tower : Seoul-VPC-HQ
- Production Workload : Seoul-VPC-PRD
- Staging Workload : Seoul-VPC-STG
- Dev Workload : Seoul-VPC-Dev

2. STG, DEV 간의 개발 작업 종료 후 잦은 네트워크 연결이 필요합니다.

3. STG, DEV 완료 후에 잠시 동안 PRD와 연결이 필요합니다.

4. PRD 가 개시되기 직전에 인터넷을 차단하고, HQ를 통해서 인터넷에 연결되며 보안을 강화합니다.

목표 구성과 필요작업은 아래와 같습니다.



## Task9. Staging과 Dev 연결

Seoul-VPC-STG와 Seoul-VPC-DEV를 TGW를 통해 연결 구성해 봅니다.

East-To-West에는 이미 Seoul-VPC-STG, Seoul-VPC-DEV의 CIDR가 Propagated 되어 있기 때문에, TGW에서 작업은 불필요합니다. 하지만 각 VPC에서 라우팅 테이블이 구성되어 있지 않기 때문에 상호간 연결되지 않습니다.

아래 명령을 통해 각 Cloud9 터미널 콘에서 Ping 시험을 해 봅니다.

**i** Cloudfomation을 통해 Security Group은 시험에 필요한 트래픽은 모두 허용되어 있습니다.

```

1 ##Seoul-VPC-STG-Private-10.2.21.101
2 ping SEOUL-VPC-DEV-Private
3

```

```

1 ##Seoul-VPC-DEV-Private-10.3.21.101
2 ping SEOUL-VPC-STG-Private

```

**i** 상호간의 트래픽이 허용되지 않습니다. 각 VPC에서 라우팅 테이블이 없기 때문입니다.

VPC- 가상 프라이빗 클라우드 - 라우팅 테이블에서 아래 라우팅 테이블 Tag 확인하고, 수정합니다.

### Seoul-VPC-STG-Private-Subnet-A-RT

Name	라우팅 테이블 ID	명시적으로 다음과 연결	Edge associations	기본	VPC ID
Seoul-VPC-STG-Private-Subnet-A-RT	rtb-005bab03836a598b2	subnet-0e9f6ba41f8e7b08a	-	아니요	vpc-05e0d6104d2a57256   Seoul-VPC-STG
라우팅 테이블: rtb-005bab03836a598b2					
요약	라우팅	서브넷 연결	Edge Associations	라우팅 전파	태그
<b>라우팅 편집</b>					
보기	모든 라우팅	<b>10.0.0.0/8 의 목적지를 생성한 TGW로 향하도록 추가합니다.</b>			
대상	대상	상태	전파됨		
10.2.0.0/16	local	active	아니요		
0.0.0.0/0	nat-0b20e5aaac91f4039	active	아니요		
10.0.0.0/8	tgw-0408d8883c27453ea	active	아니요		

### Seoul-VPC-DEV-Private-Subnet-A-RT

Name	라우팅 테이블 ID	명시적으로 다음과 연결	Edge associations	기본	VPC ID
Seoul-VPC-DEV-Private-Subnet-A-RT	rtb-09961adcf8cc8601	subnet-02ed8e01dc8d3de06	-	아니요	vpc-0e45aab6bde0ec03   Seoul-VPC-DEV
라우팅 테이블: rtb-09961adcf8cc8601					
요약	라우팅	서브넷 연결	Edge Associations	라우팅 전파	태그
<b>라우팅 편집</b>					
보기	모든 라우팅	<b>10.0.0.0/8 의 목적지를 생성한 TGW로 향하도록 추가합니다.</b>			
대상	대상	상태	전파됨		
10.3.0.0/16	local	active	아니요		
0.0.0.0/0	nat-01bec53477a65bb21	active	아니요		
10.0.0.0/8	tgw-0408d8883c27453ea	active	아니요		

이제 다시 앞서 실행한 각 인스턴스에서의 Ping이 정상적으로 처리되는지 확인합니다.



이제 Dev환경에서 Stage환경으로 연결이 되었습니다.

## Task10. Production 연결

Dev, Stage 환경에서 모든 준비가 완료되고 필요 요구에 따라 Production으로 연결이 필요하게 되었습니다.

앞서 Task7과 유사하게 Production에서 라우팅 테이블만 변경하면 Production, Staging, Dev는 모두 연결 됩니다.

아래 명령을 통해 각 Cloud9 터미널 콘솔에서 Ping 시험을 해 봅니다.



Cloudformation을 통해 Security Group은 시험에 필요한 트래픽은 모두 허용되어 있습니다.

```
1 ##Seoul-VPC-PRD-Private-10.1.21.101
2 ping SEOUL-VPC-DEV-Private
3
```

```
1 ##Seoul-VPC-PRD-Private-10.1.21.101
2 ping SEOUL-VPC-STG-Private
```



상호간의 트래픽이 허용되지 않습니다. 각 VPC에서 라우팅 테이블이 없기 때문입니다.

VPC- 가상 프라이빗 클라우드 - 라우팅 테이블에서 아래 라우팅 테이블 Tag 확인하고, 수정합니다.

### Seoul-VPC-PRD-Private-Subnet-A-RT

대상	대상	상태	전파됨
10.1.0.0/16	local	active	아니요
0.0.0.0/0	nat-0bef0dddee595aa628	active	아니요
10.0.0.0/8	tgw-0408d8883c27453ea	active	아니요

이제 다시 앞서 실행한 각 인스턴스에서의 Ping이 정상적으로 처리되는지 확인합니다.



이제 Production과 Dev, Staging 환경이 연결되었습니다.



Production과 Staging 간의 10.2.21.101만 잠시 Block하고 싶습니다. 어떻게 해야 할까요?

Transit Gateway에는 Blackhole 기능이 있습니다. 이것은 전통적인 네트워크 장비에서 Null Routing과 유사합니다. 특정 라우팅테이블을 블랙홀에 빠뜨려서, 격리시키는 방식으로 Transit Gateway를 통과시키지 못하도록 합니다.

### VPC- TransitGateway-TransitGateway 라우팅 테이블을 선택합니다.

Seoul-TGW-RT-East-To-West RouteTable을 선택하고, Route 탭을 선택합니다.

Create Static Route 버튼을 누르고 아래와 같이 Staging Host만 격리 시켜 봅니다.

```
1 ###Blockhole Target host  
2 10.2.21.101/32
```

## Create static route

Add a static route to your Transit Gateway route table.

Transit Gateway ID tgw-0408d8883c27453ea

Transit Gateway route table ID tgw-rtb-0e0cb51fdd169e86f

CIDR\* 10.2.21.101/32

Blackhole  i

CIDR	Attachment	Resource type	Route type	Route state
10.1.0.0/16	tgw-attach-03b55a9871718d37c   vpc-0fb93a230e2505bfc	VPC	propagated	active
10.2.0.0/16	tgw-attach-0e3367ffc77a56807   vpc-05e0d6104d2a57256	VPC	propagated	active
10.2.21.101/32	-	-	static	blackhole
10.3.0.0/16	tgw-attach-0405e1b969c803e9e   vpc-0e45aab6bdedec03	VPC	propagated	active

다시 Blackhole을 해제합니다.

## Task11. Production과 HQ 연결

이제 모든 작업이 완료되고, Production 개시 단계입니다. 보안 강화를 위해 SEOUL-HQ-VPC 를 통해서 외부 연결을 하도록 합니다.

먼저 TGW East-To-West 라우팅테이블에 아래와 같이 Seoul-VPC-HQ로 트래픽 경로를 추가합니다.

VPC-Transit Gateway-Transit Gateway 라우팅테이블 을 선택합니다.

Seoul-TGW-RT-East-To-West 를 선택하고, Route 탭을 선택합니다.

Create Static Route 를 선택하고, 0.0.0.0/0에 대한 경로를 Seoul-TGW-Seoul-VPC-HQ Attachment 추가합니다.

### Create static route

Add a static route to your Transit Gateway route table.

Transit Gateway ID tgw-0408d8883c27453ea

Transit Gateway route table ID tgw-rtb-0e0cb51fdd169e86f

CIDR\* 0.0.0.0/0 

Blackhole  

0.0.0.0/0 Default Route를 HQ로 향하게 합니다.

Choose attachment  

\* 필수 사항

속성별 필터						
Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Association route table	
tgw-attach-03b55a9871718d37c	Seoul-TGW-Attach-Seoul-VPC-PRD	vpc-0fb93a230e2505bfc	vpc	606879168280	tgw-rtb-0e0cb51fdd169e86f	
tgw-attach-0405e1b969c803e9e	Seoul-TGW-Attach-Seoul-VPC-DEV	vpc-0e45aab6bdedec03	vpc	606879168280	tgw-rtb-0e0cb51fdd169e86f	
<b>tgw-attach-085547c8aa4620ef8</b>	<b>Seoul-TGW-Attach-Seoul-VPC-HQ</b>	<b>vpc-0f998522f59c79768</b>	<b>vpc</b>	<b>606879168280</b>	<b>tgw-rtb-0006f933726970080</b>	
tgw-attach-0e3367ffc77a56807	Seoul-TGW-Attach-Seoul-VPC-STG	vpc-05e0d6104d2a57256	vpc	606879168280	tgw-rtb-0e0cb51fdd169e86f	

Transit Gateway Route Table: tgw-rtb-0e0cb51fdd169e86f

Details Associations Propagations Prefix list references Routes Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create static route Replace static route Delete static route

속성별 필터 또는 키워드 검색

<input type="checkbox"/> CIDR	Attachment	Resource type	Route type	Route state	Prefix List ID
<input type="checkbox"/> 0.0.0.0/0	tgw-attach-085547c8aa4620ef8   vpc-0f998522f59c79768	VPC	static	active	-
<input type="checkbox"/> 10.1.0.0/16	tgw-attach-03b55a9871718d37c   vpc-0fb93a230e2505bfc	VPC	propagated	active	-
<input type="checkbox"/> 10.2.0.0/16	tgw-attach-0e3367ffc77a56807   vpc-05e0d6104d2a57256	VPC	propagated	active	-
<input type="checkbox"/> 10.3.0.0/16	tgw-attach-0405e1b969c803e9e   vpc-0e45aab6bdedec03	VPC	propagated	active	-

이제 Seoul-VPC-PRD의 Private Subnet 라우팅에서 인터넷으로 가는 목적지를 NAT Gateway에서 Transit Gateway로 아래와 같이 변경합니다.

Seoul-VPC-PRD-Private-Subnet-A-RT

Name	라우팅 테이블 ID	명시적으로 다음과 연결	Edge associations	기본	VPC ID
Seoul-VPC-PRD-Private-Subnet-A-RT	rtb-0a1643bf66f6559ef	subnet-05ab104f192b991ca	-	아니요	vpc-0fb93a230e2505bfc   Seoul-VPC-PRD
라우팅 테이블: rtb-0a1643bf66f6559ef					
요약	라우팅	서브넷 연결	Edge Associations	라우팅 전파	태그
라우팅 편집					
보기	모든 라우팅				
대상	대상	상태	전파됨		
10.1.0.0/16	local	active	아니요		
0.0.0.0/0	tgw-0408d8883c27453ea	active	아니요		

**Seoul-VPC-PRD-Private-10.1.21.101 인스턴스에서 www.aws.com 으로 ping을 실행해 봅니다.**

**!** 실행되지 않습니다. 이유는 간단합니다. Return 되는 경로가 Seoul-VPC-HQ에서 설정되어 있지 않습니다. NAT Gateway가 있는 Public Routing Table에서 Seoul-VPC-PRD-Private 에 대한 라우팅 경로를 추가해야 합니다. 또한 Seoul-VPC-HQ 가 연결되어 있는 Transit Gateway North-To-South에서 라우팅도 추가를 하면 정상적으로 연결됩니다.

**VPC- 가상 프라이빗 클라우드 - 라우팅 테이블**에서 아래 라우팅 테이블 Tag 확인하고, 수정합니다.

### Seoul-VPC-HQ-PublicRT

Name	라우팅 테이블 ID	명시적으로 다음과 연결	Edge associations	기본	VPC ID
Seoul-VPC-HQ-PublicRT	rtb-080fdc5a24967079a	2개의 서브넷	-	아니요	vpc-0f998522f59c79768   Seoul-VPC-HQ
라우팅 테이블: rtb-080fdc5a24967079a					
요약	라우팅	서브넷 연결	Edge Associations	라우팅 전파	태그
라우팅 편집					
보기	모든 라우팅				
대상	대상	상태	전파됨		
10.0.0.0/16	local	active	아니요		
0.0.0.0/0	igw-0ec1584e46ba8cc4e	active	아니요		
10.1.21.0/24	tgw-0408d8883c27453ea	active	아니요		

TGW North-To-South 라우팅테이블에 아래와 같이 Seoul-VPC-HQ로 트래픽 경로를 추가합니다.

VPC-Transit Gateway-Transit Gateway 라우팅테이블 을 선택합니다.

Seoul-TGW-RT-North-To-South 를 선택하고, Route 탭을 선택합니다.

Create Static Route 를 선택하고, 10.1.21.0/24 에 대한 경로를 Seoul-TGW-Seoul-VPC-PRD Attachment 추가합니다.

The screenshot shows the AWS CloudFormation console interface for managing Transit Gateway routes. At the top, there is a search bar labeled '태그 및 속성별 필터 또는 키워드별 검색'. Below it is a table with columns: Name, Transit Gateway route table ID, Transit Gateway ID, State, Default association route table, and Default propagation route table. Three rows are listed:

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
Seoul-TGW-RT-North-To-South	tgw-rb-0006f933726970080	tgw-0408d8883c27453ea	available	No	No
Seoul-TGW-RT-East-To-West	tgw-rb-0e0cb51fd169e86f	tgw-0408d8883c27453ea	available	No	No
	tgw-rb-00580867329736172	tgw-0427a45e96fc9bff2	available	Yes	Yes

Below the table, a message says 'Transit Gateway Route Table: tgw-rb-0006f933726970080'. Underneath are tabs: Details, Associations, Propagations, Prefix list references, Routes (which is selected), and Tags. A note below the tabs states: 'The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.' There are three buttons: Create static route (highlighted in blue), Replace static route, and Delete static route. The 'Routes' section table has columns: CIDR, Attachment, Resource type, Route type, Route state, and Prefix List ID. Two routes are listed:

CIDR	Attachment	Resource type	Route type	Route state	Prefix List ID
10.0.0.0/16	tgw-attach-085547c8aa4620ef8   vpc-0f998522f59c79768	VPC	propagated	active	-
10.1.21.0/24	tgw-attach-03b55a9871718d37c   vpc-0fb93a230e2505bfc	VPC	static	active	-

이제 Seoul-VPC-PRD-Private-10.1.21.101 인스턴스에서 정상적으로 외부 접속이 되는지 확인해 봅니다.



Transit Gateway 구성에 대한 모든 실습을 마쳤습니다. 연결되는 다음 Chapter를 사용하지 않을 경우, Cloudformation에서 Stack을 **Seoul-TGW.yml** 부터 삭제하고, 나머지 VPC yml을 삭제하면 모든 자원이 삭제 됩니다.

## TransitGateway 구성하기 과정

### 1.4개의 VPC 생성

- Cloudformation을 통해서, 다운로드 받은 4개의 yaml 파일 업로드 (Seoul-VPC-HQ, Seoul-VPC-PRD, Seoul-VPC-STG, Seoul-VPC-DEV)하고 , VPC 생성

## 2. 서울 리전(ap-northeast-2)에서 TransitGateway 생성

- Cloudformation을 통해서, 다운로드 받은 yaml 파일 업로드(Seoul-TGW)하고, TGW 생성

## 3. 생성된 VPC, EC2 구성 확인.

## 4. TGW 구성확인

## 5. TGW Attachment (연결) 확인

## 6. TGW Routing Table 확인

## 7. Session Manager를 통해서 EC2 인스턴스 접속하기

## 8. 시나리오 이해하기

## 9. Staging VPC와 Dev VPC 연결하기 - TGW를 통해 연결하

## 10. Production 연결하기 - TGW 연결하기.

## 11. Production과 HQ 연결하기 - 서로 다른 라우팅 테이블에서 연결하기.

해당 LAB의 질문 사항은 [whchoi98@gmail.com](mailto:whchoi98@gmail.com)/ [whchoi@amazon.com](mailto:whchoi@amazon.com) 또는  [슬랙채널](#) (<https://whchoi-hol.slack.com/archives/C01QM79Q4BD>)에서 문의 가능합니다.

# Transit Gateway MultiAccount

## 1. Transit Gateway MultiAccount 연결

### 개요

Transit Gateway는 동일 리전에서 서로 다른 계정에서 Transit Gateway Peering을 사용할 수 없습니다.

예를 들어 빌더스 컴퍼니와 협력사인 서밋 컴퍼니는 상호간에 Transit Gateway Peering을 동일 리전에서 연결할 수 없습니다. 이러한 경우 RAM(Resource Access Manager)를 통해서 간단하게 연결할 수 있는 디자인을 제공하고 있습니다.

아래와 같이 서울 리전안에서 2개의 계정간에 개발 협력을 위해 연결하는 과정을 소개합니다.

### RAM (Resource Access Manager) 소개

AWS Resource Access Manager (RAM)은 AWS 계정 또는 AWS 조직 내에서 AWS 리소스를 쉽고 안전하게 공유 할 수 있는 서비스입니다. AWS Transit Gateway, 서브넷, AWS License Manager 구성 및 Amazon Route 53 Resolver 규칙 리소스를 RAM과 공유 할 수 있습니다.

많은 조직은 관리 또는 비용처리에 대한 부분에 대해 상호간의 영향 제한하기 위해 여러 계정을 사용합니다. RAM을 사용하면 여러 계정에 중복 리소스를 만들 필요가 없으므로 소유 한 모든 단일 계정에서 해당 리소스를 관리하는 운영 오버 헤드가 줄어 듭니다. 여러개 계정 환경에서 중앙 집중식으로 리소스를 생성하고 RAM을 사용하여 리소스 공유 생성, 리소스 지정 및 계정 선이라는 세 가지 간단한 단계로 계정간에 해당 리소스를 공유 할 수 있습니다. RAM은 추가 비용없이 사용할 수 있습니다.

RAM을 사용하면 다음과 같은 장점이 있습니다.

### 운영 오버 헤드 감소

중앙에서 AWS 리소스를 조달하고 RAM을 사용하여 서브넷 또는 라이선스 관리자 구성과 같은 리소스를 다른 계정과 공유합니다. 이렇게하면 다중 계정 환경의 모든 계정에 중복 리소스

를 프로비저닝 할 필요가 없으므로 모든 계정에서 해당 리소스를 관리하는 운영 오버 헤드가 줄어 듭니다.

## 보안 및 가시성 향상

RAM은 AWS Identity and Access Management (IAM)에 설정된 기존 정책과 권한을 활용하여 공유 리소스의 사용을 관리합니다. RAM은 또한 Amazon CloudWatch 및 AWS CloudTrail과의 통합을 통해 알람을 설정하고, 로그를 시각화하기 위해 공유 리소스에 대한 포괄적 인가시성을 제공합니다.

## 비용 최적화

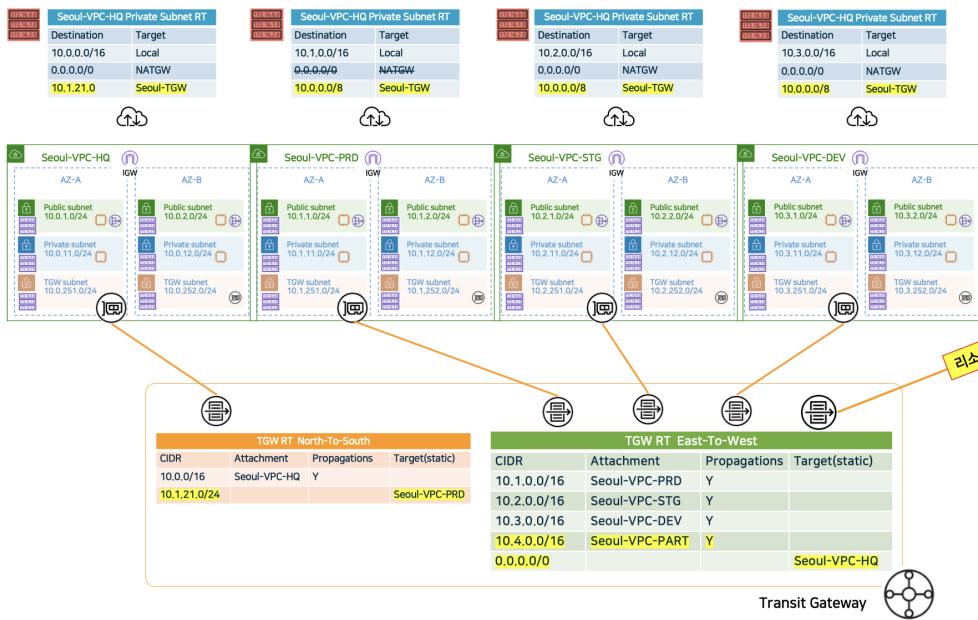
계정 간에 AWS License Manager 구성과 같은 리소스를 공유하면 회사의 여러 부분에서 라이선스를 활용하여 활용도를 높이고 비용을 최적화 할 수 있습니다.

## 구성 아키텍쳐 소개

[TransitGateway 구성하기](#)에서 생성한 빌더스 컴퍼니의 Transit Gateway를 동일한 서울 리전, 다른 어카운트(서밋 컴퍼니) Seoul-VPC-PART VPC에서 사용하려고 하는 목표 구성입니다.

AWS RAM(Resource Access Manager)를 이용하여 빌더스 컴퍼니의 Transit Gateway를 연계 해서, 협력사인 서밋 컴퍼니 자원을 사용해 봅니다.

## Account : 빌더스 컴퍼니



## Account : 서밋 컴퍼니



## 2. 서로 다른 계정에서 TGW 연동

### Task 1. VPC 구성하기

새로운 계정에 접속하고, Cloudformation을 통해 기본이 되는 VPC구성을 먼저 구성합니다.

#### 1. 사전 준비하기

서울 리전에 4개의 VPC를 구성하고, 사전에 구성된 TGW를 배포합니다.

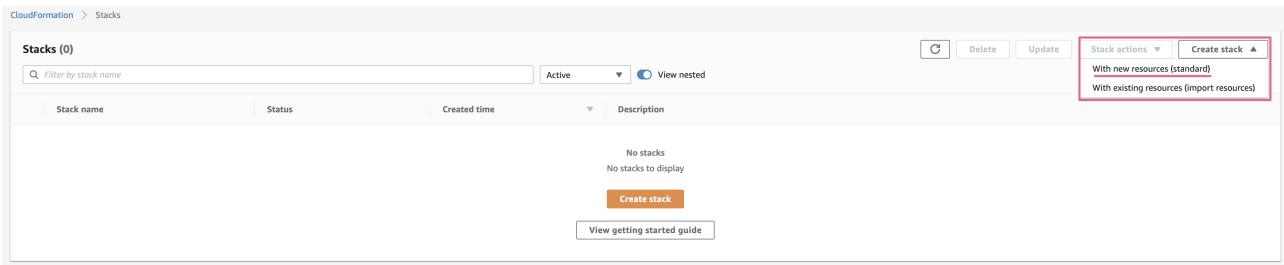
아래 Github에서 실습에 사용할 Cloudformation yaml 파일을 다운로드 받습니다. (이미 받았다면 생략합니다.)

```
git clone https://github.com/whchoi98/builders20210312
```

#### 2. Cloudformation 생성.

**!** 서밋 컴퓨터는 서울리전에서 새로운 계정을 Seoul-VPC-PART라는 이름으로 VPC를 생성합니다.

Seoul-VPC-PART 를 Cloudformation 을 기반으로 생성합니다.

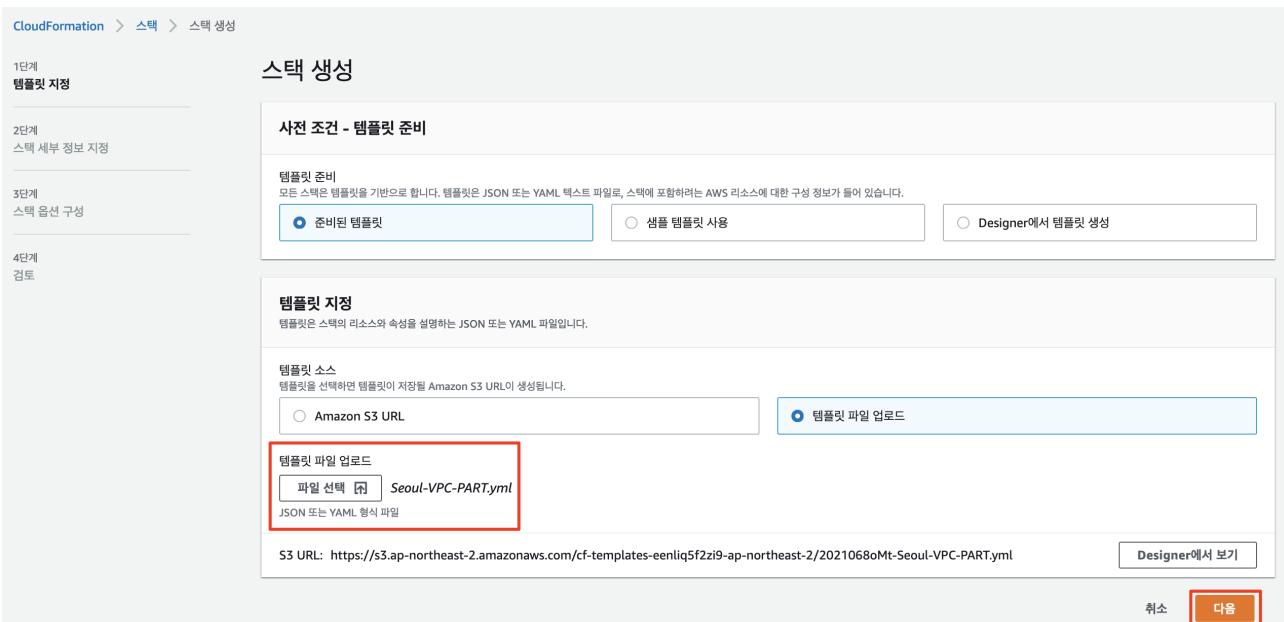


AWS 콘솔에서 서울 리전 (ap-northeast-2)를 선택하고, Cloudformation 서비스를 선택합니다.

Cloudformation에서 먼저 새로운 스택을 생성합니다.

앞서 다운로드 받은 yaml 파일들 중에 Seoul-VPC-PART.yaml 파일을 업로드 합니다.

Seoul-VPC-PART.yaml



다음을 선택하고, 아래와 같아 스택이름은 파일명과 동일하게 입력합니다.

### 스택 세부 정보 지정

스택 이름

스택 이름  
Seoul-VPC-PART

스택 이름은 문자(A-Z 및 a-z), 숫자(0-9) 및 대시(-)를 포함할 수 있습니다.

별도로 설정 변경없이, 다음 단계를 진행하고, 승인을 선택하고 스택생성합니다.

▶ 빠른 생성 링크

기능

**ⓘ The following resource(s) require capabilities: [AWS::IAM::InstanceProfile, AWS::IAM::Role]**

이 템플릿에는 자격 증명 및 액세스 관리(IAM) 리소스가 들어 있습니다. 각 리소스를 생성할 것인지 그리고 그러한 리소스가 필요한 최소 권한을 가지고 있는지 확인합니다. 또한 이러한 리소스는 사용자 지정 이름을 가집니다. 사용자 지정 이름이 해당 AWS 계정에서 고유한지 확인합니다. 자세히 알아보기 [\[?\]](#)

AWS CloudFormation에서 사용자 지정 이름으로 IAM 리소스를 생성할 수 있음을 승인합니다.

취소 이전 변경 세트 만들기 **스택 생성**

정상적으로 구성되면 아래와 같이 Cloudformation에서 확인 할 수 있습니다. VPC는 각 3분 내외에 생성됩니다.

CloudFormation > 스택 > Seoul-VPC-PART

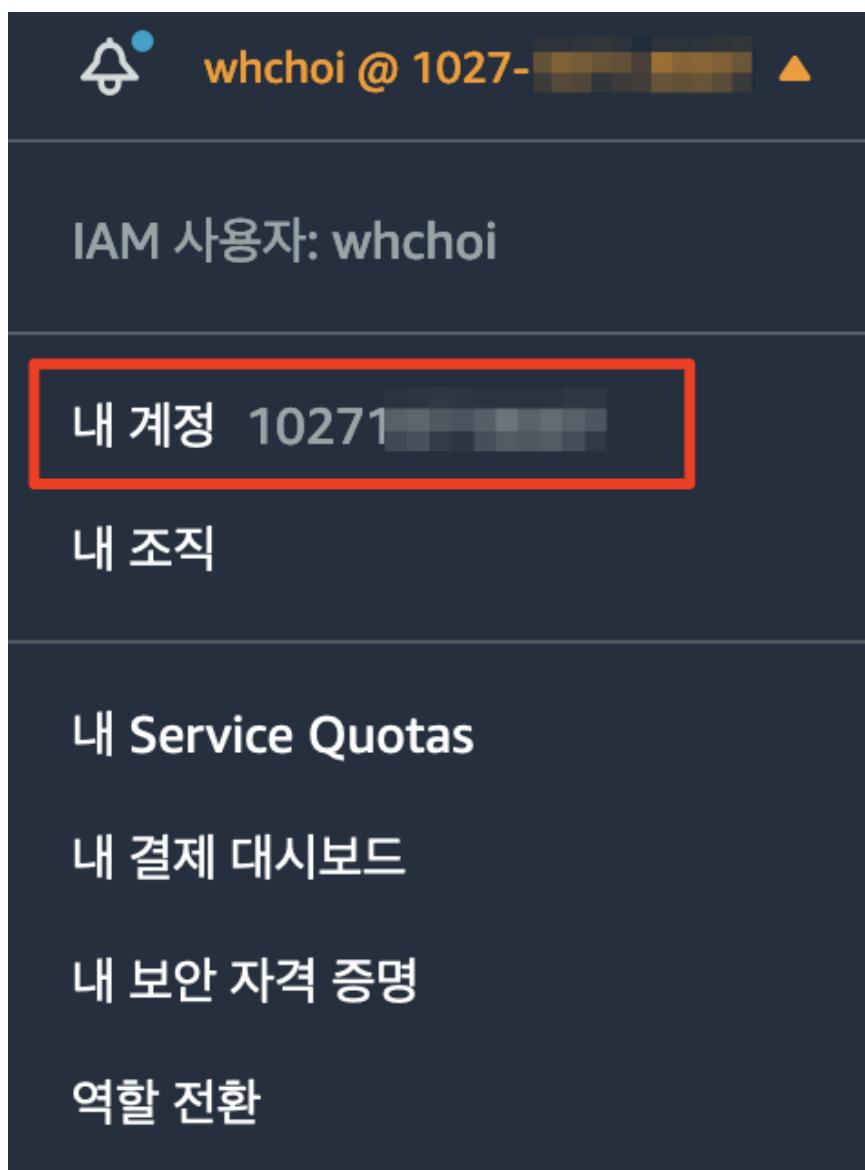
### ▣ 스택 (3)

스택 이름으로 필터링

활성 ▾ 뷰 중첩됨 < 1 >

Seoul-VPC-PART 2021-03-09 13:48:18 UTC+0900 <b>CREATE_COMPLETE</b>
--

서밋 컴퍼니 계의 번호를 복사해 둡니다. RAM 구성시 계정 정보가 필요합니다.



## Task 2. RAM 구성하기

이제 다시 빌더스 컴퍼니 계정에서 수행합니다.

- ⓘ 빌더스 컴퍼니에서 생성된 TGW를 서밋 컴퍼니에게 제공할 것입니다. 반드시 RAM 구성은 리소스 제공하는 계정에서 실행합니다.

AWS 관리콘솔에서 RAM 을 선택하고, 새로운 윈도우 창을 오픈합니다.

A screenshot of the AWS RAM search results. The search bar at the top contains the text 'RAM'. Below the search bar, the results are listed under the heading '서비스' (Services). There are two services listed: 'Resource Access Manager' and 'Amazon CloudWatch Metrics'. The 'Resource Access Manager' entry is highlighted with a red border. To the left of the main results, there are filters for '서비스 (2)', '기능 (4)', '설명서 (28,101)', and '마켓플레이스 (35)'. The 'Resource Access Manager' entry includes a small icon, the service name, a description ('다른 계정 또는 AWS Organizations와 AWS 리소스 공유'), and a '선택' (Select) button.

Resource Access Manager - 내가 공유: 리소스 공유에서 "리소스 공유 생성"을 선택합니다.

A screenshot of the 'Create Resource Share' page in the Resource Access Manager. The page title is '내가 공유: 리소스 공유'. On the left, there is a sidebar with a single item: '리소스 공유 (1)' (1 resource share). The main content area shows a table with one row, which is highlighted with a red border. The table columns are 'Name' (Name), 'AWS Organizations 팀' (AWS Organizations Team), and '선택' (Select). The '선택' column for the first row contains a red-bordered '리소스 공유 생성' (Create Resource Share) button. At the bottom of the page, there is a search bar and navigation controls.

아래와 값을 입력합니다.

- **이름** - "리소스 공유 이름"을 입력합니다.

A screenshot of a dark blue input field containing the text 'Seoul-TGW'. This is likely a placeholder or a suggested value for the 'Resource Share Name' field.

- **리소스 유형 선택** - 전송 게이트웨이 (Transit Gateway)를 선택하고, 생성해 놓은 TGW를 선택합니다.
- **Principal** - 외부 계정 허용을 선택합니다. 앞서 새롭게 Seoul-VPC-PART VPC 자원이 생성된 계정의 번호를 입력합니다. (앞서 복사해 둔 서밋 컴퍼니의 계정입니다.)

Resource Access Manager > 내가 공유 : 리소스 공유 > 리소스 공유 생성

### 리소스 공유 생성

리소스 공유를 생성하여 AWS 계정, 조직 단위 또는 조직에 리소스 액세스 권한 제공

**설명**

이름  
리소스 공유에 설명이 포함된 이름 지정  
**리소스 공유 이름**  
Seoul-TGW

**리소스 - 선택 사항**  
리소스 공유에 추가할 리소스 선택

리소스 유형 선택  
전송 케이트웨이 **리소스 유형 선택**

속성 필터 또는 키워드별 검색

ID	리소스 선택	이름	설명	상태
<input checked="" type="checkbox"/> tgw-0408d8883c27453ea	TGW 선택	Seoul-TGW	TGW Route Integration Test	available
<input type="checkbox"/> tgw-0427a45e9efc9bf2		-	-	available

선택 리소스  
tgw-0408d8883c27453ea

**프린시펄 - 선택 사항**  
리소스 공유에 프린시펄을 추가합니다. 프린시펄은 AWS 계정, 조직 단위 또는 조직일 수 있습니다.

외부 계정 허용 정부  
조직 외부의 다른 AWS 계정에 액세스

AWS 계정 번호, OU 또는 조직 추가  
선택한 프린시펄  
10271 [ ] AWS 계정

리소스 공유를 확인하고, 생성한 리소스 공유를 선택합니다.

Resource Access Manager > 내가 공유 : 리소스 공유

### 리소스 공유 (2)

내 계정이 소유하는 리소스 공유

ID	소유자	외부 프린시펄 허용	상태
<input type="radio"/> TGW-RAM	fbaea24d-6420-4e8e-b345-d1c12f4ab22b	예	<input type="radio"/> Deleted
<input type="radio"/> Seoul-TGW	fd4a9c06-3976-466e-bc8f-108dc04f1bc	예	<input checked="" type="radio"/> Active

Associating 단계로 진행 중인 것을 확인 할 수 있습니다.

공유한 프린시펄 (1)

프린시펄 ID	프린시펄 유형	상태
1027 [ ]	계정 (외부)	<b>① Associating 보기.</b>

이제 공유를 확인하기 위해, 협력사인 서밋 컴퍼니 계정 콘솔로 이동해서 RAM으로 이동합니다.

서밋 컴퍼니 - AWS 계정 - RAM 을 선택합니다.

리소스 공유에 초대 알람이 생성된 것을 확인 할 수 있습니다. 리소스 공유를 선택합니다.

**AWS Resource Access Manager**

**초대 메세지**

다른 AWS 계정과 AWS 리소스를 공유합니다.

**작동 방식**

리소스 공유 1 초대

공유 리소스

프린시펄

설정

해당 리소스 공유를 선택하면, 리소스 공유 수락을 대기하고 있는 것을 확인 할 수 있습니다.  
공유된 리소스 Seoul-TGW 를 선택합니다.

Resource Access Manager > 나의 공유 : 리소스 공유

리소스 공유 (1 selected)

내 계정이 액세스하는 리소스 공유

속성별 필터 또는 키워드별 검색

이름	ID	소유자	상태
Seoul-TGW	fd4a9c06-3976-466e-bc8f-108dc04f1bcb	606879168280	Pending

리소스 공유 수락을 선택합니다.

Resource Access Manager > 나의 공유 : 리소스 공유 > 리소스 공유 fd4a9c06-3976-466e-bc8f-108dc04f1bcb

Seoul-TGW (fd4a9c06-3976-466e-bc8f-108dc04f1bcb)

이 리소스 공유에 관한 세부 정보 및 정보

리소스 공유 거부 리소스 공유 수락

리소스 공유를 수락합니다.

요약

이름 Seoul-TGW	소유자 606879168280	최대 날짜 2021/03/09	상태 Pending
ARN arn:aws:ram:ap-northeast-2:606879168280:resource-share/fd4a9c06-3976-466e-bc8f-108dc04f1bcb			

AWS 계정 - VPC - TransitGateway에 빌더스 컴퍼니 계정의 Seoul-TGW가 나타납니다.

Tags 및 속성별 필터 또는 키워드별 검색

Name	Transit Gateway ID	Owner ID	State
	tgw-0408d8883c27453ea	606879168280	available

Transit Gateway: tgw-0408d8883c27453ea

Details Tags Sharing

Transit Gateway ID	tgw-0408d8883c27453ea	Owner account ID	606879168280 (shared)
State	available	Amazon ASN	65001
DNS support	enable	VPN ECMP support	enable
Auto accept shared attachments	enable	Default association route table	disable
Association route table ID	-	Default propagation route table	disable
Propagation route table ID	-	Multicast support	disable

## Task 3. TGW 연동하기

서밋 컴퍼니 계정에서 Transit Gateway Attachment를 생성하기 위해,

**VPC – Transit Gateway – Transit Gateway 연결** 을 선택해서 새로운 Attachment를 생성합니다.

- Transit Gateway ID : 공유된 TGW
- Attachment name tag : Attachment 이름 (Seoul-TGW-Attach-Seoul-VPC-PART)
- VPC ID : 서밋 컴퍼니의 VPC 선택 (Seoul-VPC-PART)
- Subnet : TGW ENI가 연결된 서브넷 선택 (Seoul-VPC-TGWSUBNETA, Seoul-VPC-TGWSUBNETB)

[Transit Gateway Attachments](#) > Create Transit Gateway Attachment

### Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID\* tgw-0408d8883c27453ea C **공유된 TGW**

Attachment type VPC C i

#### VPC Attachment

Select and configure your VPC attachment.

Attachment name tag Seoul-TGW-Attach-Seoul-VPC-PART i **Attachment 이름**

DNS support  enable i

IPv6 support  enable i

VPC ID\* vpc-0bc575f2c1cbe8e20 C **생성한 VPC**

Subnet IDs\* subnet-09adde2c56bbf0b25 x subnet-0dc6e7fc4216f4aae x i

TGW ENI가 생성될 Subnet	Availability Zone	Subnet ID
	ap-northeast-2a	subnet-09adde2c56bbf0b25 (Seoul-VPC-PART-TGWSUBNETA)
	ap-northeast-2b	subnet-0dc6e7fc4216f4aae (Seoul-VPC-PART-TGWSUBNETB)

**VPC – Transit Gateway – Transit Gateway 연결** 에서 정상적으로 구성되었는지 확인합니다.

Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State	Assoc.
Seoul-TGW-Attach-Seoul-VPC...	tgw-attach-0a27b48e3e9f02a8e	tgw-0408d8883c27453ea	VPC	vpc-0bc575f2c1cbe8e20	available	-

Transit Gateway Attachment: tgw-attach-0a27b48e3e9f02a8e

Details Tags

Transit Gateway attachment ID	tgw-attach-0a27b48e3e9f02a8e	Transit Gateway owner ID	6068 [REDACTED] (shared)
Transit Gateway ID	tgw-0408d8883c27453ea	Resource owner account ID	1027 [REDACTED]
Resource type	VPC	State	available
Resource ID	vpc-0bc575f2c1cbe8e20	Associated route table	-
Association state	-	DNS support	enable
IPv6 support	disable	Subnet IDs	subnet-09adde2c56bbf0b25 subnet-0dc6e7fc4216f4aae

라우팅 테이블에서 Association을 수행합니다.

 TGW와 Routing Table 자원은 모두 빌더스 컴퍼니 계정 소유입니다. 따라서 Association, Routing Table 구성은 빌더스 계정에서 수행합니다.

이제 다시 빌더스 계정으로 이동합니다.

빌더스 계정 - AWS 콘솔 - VPC- Transit Gateway - Transit Gateway 라우팅 테이블에서 "Seoul-TGW-RT-East-To-West" 테이블을 선택합니다. 새롭게 추가된 서밋 컴퍼니 계정의 **Transit Gateway Attachment**를 선택하고 추가합니다.

Transit Gateway Route Tables > Create association

#### Create association

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated to one route table.

Transit Gateway ID tgw-0408d8883c27453ea

Transit Gateway route table ID tgw-rtb-0e0cb51fdd169e86f

Choose attachment to associate\* | C

Sectio... 필수 사용						
Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Association route table	
tgw-attach-03b55a9871718d37c	Seoul-TGW-Attach-Seoul-VPC-PRD	vpc-0fb93a2230e2505bf0	vpc	606879168280	tgw-rtb-0e0cb51fdd169e86f	
tgw-attach-0405e1b969c803e9e	Seoul-TGW-Attach-Seoul-VPC-DEV	vpc-0e45aab8bdedec03	vpc	606879168280	tgw-rtb-0e0cb51fdd169e86f	
tgw-attach-085547c8aa4620ef8	Seoul-TGW-Attach-Seoul-VPC-HQ	vpc-0f998522f59c79768	vpc	606879168280	tgw-rtb-0006f933726970080	
tgw-attach-0a27b48e3e9f02a8e		vpc-0bc575f2c1cbe8e20	vpc	102719718687		
tgw-attach-0e3367ffc77a56807	Seoul-TGW-Attach-Seoul-VPC-STG	vpc-05e0d6104d2a57256	vpc	606879168280	tgw-rtb-0e0cb51fdd169e86f	

AWS 콘솔 - VPC- Transit Gateway - Transit Gateway 라우팅 테이블 - "Seoul-TGW-RT-East-To-West" - Assosiations Tab

를 선택합니다. 정상적으로 Association 되었는지 확인합니다.

Transit Gateway Route Table: tgw-rb-0e0cb51fdd169e86f

**Associations**

**Create association**

Attachment ID	Resource type	Resource ID	State
tgw-attach-0e3367ffc77a56807	VPC	vpc-05e0d6104d2a57256	associated
tgw-attach-0a27b48e3e9f02a8e	VPC	vpc-0bc575f2c1cbe8e20	associated
tgw-attach-0405e1b969c803e9e	VPC	vpc-0e45aab6bdeec03	associated
tgw-attach-03b55a9871718d37c	VPC	vpc-0fb93a230e2505bfc	associated

## AWS 콘솔 - VPC- Transit Gateway – Transit Gateway 라우팅 테이블 – Propagations Tab

을 선택하고, 서밋 컴퍼니의 Seoul-VPC-PART 를 propagation 합니다.

Transit Gateway Route Tables > Create propagation

### Create propagation

Adding a propagation will allow routes to be propagated from an attachment to the target Transit Gateway route table. An attachment can be propagated to multiple route tables.

Transit Gateway ID tgw-0408d8883c27453ea

Transit Gateway route table ID tgw-rb-0e0cb51fdd169e86f

Choose attachment to propagate\*

속성별 필터

Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Association route table
tgw-attach-03b55a9871718d37c	Seoul-TGW-Attach-Seoul-VPC-PRD	vpc-0fb93a230e2505bfc	vpc	606879168280	tgw-rb-0e0cb51fdd169e86f
tgw-attach-0405e1b969c803e9e	Seoul-TGW-Attach-Seoul-VPC-DEV	vpc-0e45aab6bdeec03	vpc	606879168280	tgw-rb-0e0cb51fdd169e86f
tgw-attach-085547c8aa4620ef8	Seoul-TGW-Attach-Seoul-VPC-HQ	vpc-0f998522f59c79768	vpc	606879168280	tgw-rb-0006f933726970080
tgw-attach-0a27b48e3e9f02a8e		vpc-0bc575f2c1cbe8e20	vpc	10271971887	tgw-rb-0e0cb51fdd169e86f
tgw-attach-0e3367ffc77a56807	Seoul-TGW-Attach-Seoul-VPC-STG	vpc-05e0d6104d2a57256	vpc	606879168280	tgw-rb-0e0cb51fdd169e86f

## AWS 콘솔 - VPC- Transit Gateway – Transit Gateway 라우팅 테이블 – Propagations Tab

을 선택하고, 정상적으로 Propagation 되었는지 확인합니다.

Transit Gateway Route Table: tgw-rtb-0e0cb51fdd169e86f

Details Associations Propagations Prefix list references Routes Tags

Create propagation Delete propagation

Attachment ID	Resource type	Resource ID	State
tgw-attach-03b55a9871718d37c	VPC	vpc-0fb93a230e2505bfc	enabled
tgw-attach-0405e1b969c803e9e	VPC	vpc-0e45aab6bdedeeec03	enabled
<b>tgw-attach-0a27b48e3e9f02a8e</b>	VPC	vpc-0bc575f2c1cbe8e20	enabled
tgw-attach-0e3367ffc77a56807	VPC	vpc-05e0d6104d2a57256	enabled

AWS 콘솔 - VPC- Transit Gateway - Transit Gateway 라우팅 테이블 - Route Tab 을 선택하고, 정상적으로 Route가 추가되었는지 확인합니다.

Transit Gateway Route Table: tgw-rtb-0e0cb51fdd169e86f

Details Associations Propagations Prefix list references **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create static route Replace static route Delete static route

CIDR	Attachment	Resource type	Route type	Route state	Prefix List
0.0.0.0/0	tgw-attach-085547c8aa4620ef8   vpc-0f998522f59c79768	VPC	static	active	-
10.1.0.0/16	tgw-attach-03b55a9871718d37c   vpc-0fb93a230e2505bfc	VPC	propagated	active	-
10.2.0.0/16	tgw-attach-0e3367ffc77a56807   vpc-05e0d6104d2a57256	VPC	propagated	active	-
10.3.0.0/16	tgw-attach-0405e1b969c803e9e   vpc-0e45aab6bdedeeec03	VPC	propagated	active	-
<b>10.4.0.0/16</b>	<b>tgw-attach-0a27b48e3e9f02a8e   vpc-0bc575f2c1cbe8e20</b>	VPC	propagated	active	-

서밋 컴퓨터 계정에서 SEOUL-VPC-PRT-Private-10.4.21.101 을 접속합니다.

SEOUL-VPC-PRT-Private-10.4.21.101 id 확인.

계정이 2개 구성되어 aws cli는 default profile로 접근이 됩니다. 아래와 같이 2개의 구성을 관리자 PC 또는 리눅스에서 설정합니다.

```

1 ~/aws/config
2 [profile builders]
3 region = ap-northeast-2
4 output = json
5 [profile summit]
```

```
6 region = ap-northeast-2
7 output = json
8
9 ~/.aws/credentials
10 [builders]
11 aws_access_key_id = xxxxxxx
12 aws_secret_access_key = xxxxx
13 [summit]
14 aws_access_key_id = xxxxxxx
15 aws_secret_access_key = xxxxx
```

환경설정을 아래와 같이 스위칭하면서 연결합니다.

```
1 ###builders 계정
2 export AWS_DEFAULT_PROFILE=builders
3
4 ##summit 계정
5 export AWS_DEFAULT_PROFILE=builders
```

아래와 같이 Seoul-VPC-PART-Private-10.4.21.101 인스턴스 id를 조회합니다.

```
~/environment/buildernet/aws_ec2_ext.sh | grep "Seoul-VPC-PART-Private-10.4
```

Seoul-VPC-PART-Private-10.4.21.101 인스턴스에 접속합니다.

```
aws ssm start-session --target "Seoul-VPC-PART-Private-10.4.21.101 id"
```

아래 명령어를 통해 Seoul-VPC-DEV,STG 의 인스턴스로 연결이 가능한지 확인합니다.

```
1 sudo -s
2 echo 10.0.21.101 SEOUL-VPC-HQ-Private >> /etc/hosts
3 echo 10.1.21.101 SEOUL-VPC-PRD-Private >> /etc/hosts
4 echo 10.2.21.101 SEOUL-VPC-STG-Private >> /etc/hosts
5 echo 10.3.21.101 SEOUL-VPC-DEV-Private >> /etc/hosts
```

```
6 echo 10.4.21.101 SEOUL-VPC-PRT-Private >> /etc/hosts  
7 echo 10.5.21.101 IAD-VPC-Private >> /etc/hosts  
8 ping SEOUL-VPC-DEV-Private  
9
```

이제 Seoul-VPC-PART에서 Seoul-VPC-DEV, Seoul-VPC-STG로 통신을 하기 위해, 10.0.0.0/8의 목적지를 Transit Gateway로 추가합니다.

Name	리우팅 테이블 ID	명시적으로 다음과 연결	Edge associations	기본	VPC ID	소유자
Seoul-VPC-PART-Private-Subnet-A-RT	rtb-0c7db0861d1f8b806	subnet-002e0c768e75fb3a5	-	아니요	vpc-0bc575f2c1cbe8e20   ...	1027 [redacted]

리우팅 테이블: rtb-0c7db0861d1f8b806

요약 라우팅 서브넷 연결 Edge Associations 라우팅 전파 태그

라우팅 편집

보기 모든 라우팅

대상	대상	상태	전파됨
10.4.0.0/16	local	active	아니요
0.0.0.0/0	nat-05bd2cceaa550399fb	active	아니요
10.0.0.0/8	tgw-0408d8883c27453ea	active	아니요

- (i) Seoul-VPC-PART에서 Seoul-VPC-PRD로도 접근이 가능할 것입니다. 모든 VPC에서 10.0.0.0/8의 목적지를 TGW로 구성했기 때문입니다. 보안 강화를 이러한 경우에는 VPC들의 CIDR을 Propagation하지 않고, Static으로 처리하면 접근 제어가 가능합니다.

이제 Seoul-VPC-PART-Private-10.4.21.101에서 DEV, STG로 트래픽을 체크를 해보세요. PRD도 확인해 보세요.

```
1 ping SEOUL-VPC-DEV-Private  
2 ping SEOUL-VPC-STG-Private  
3 ping SEOUL-VPC-PRD-Private
```

- (✓) MultiAccount의 같은 리전에서 TGW 연동을 확인해 보았습니다. Propagation과 Static 조합을 통해서 VPC 격리와 보안을 강화하는 여러가지 디자인을 구성해 볼 수 있습니다.

---

해당 LAB의 질문 사항은 whchoi98@gmail.com/ whchoi@amazon.com 또는  슬랙채널 (<https://whchoi-hol.slack.com/archives/C01QM79Q4BD>)에서 문의 가능합니다.

# TransitGateway Peering

## 1. Transit Gateway Peering

### 개요

Transit Gateway는 서로 다른 리전에서 동일한 Transit Gateway를 사용할 수 없습니다. 서로 다른 리전은 서로 다른 TGW를 구성해야 하고, 상호 연결을 위해서는 Transit Gateway Peering을 사용해야 합니다.

이번 챕터에서는 us-east-1에서 VPC와 TGW를 생성하고 상호간에 연결 구성을 해 봅니다.

웹브라우저에서 하나의 탭을 더 열고 AWS 관리 콘솔 창 상단 우측바에서 리전을 선택하고, "us-east-1" "버지니아 북부"를 선택합니다.



서울 리전 VPC 화면 탭과 버지니아 북부 리전 VPC 화면 탭 2개를 브라우저에서 사용합니다.

## 2. EC2,VPC,TGW 구성

### Task 1. VPC 구성하기

새로운 리전(버지니아 북부 us-east-1 접속)하고, Cloudformation을 통해 기본이 되는 VPC 구성을 먼저 구성합니다.

#### 사전 준비하기

앞서 서울 리전에서 만들어 둈 keypair (public key)는 서울리전에서만 존재합니다.

us-east-1 버지니아 리전에서도 사용할 수 있도록 Cloud9 콘솔 터미널에서 아래와 같이 명령을 입력하고 서울리전의 public key를 전송합니다.

```
1  ### Converting from private key to public key
2  sudo ssh-keygen -y -f ~/environment/builders20210312.pem > ~/environment/b
3
4  ### Transfer public key to us-east-1
5  cd ~/environment
6  aws ec2 import-key-pair --key-name builders20210312 --public-key-material
7
```

정상적으로 public key가 us-east-1 리전 Keypair에 전송되었는지 확인합니다.

AWS 관리 콘솔 - EC2 - 네트워크 및 보안 - 키페어 를 클릭하고, **builders20210321** 이라는 Public key가 전송되었는지 확인합니다.

The screenshot shows the AWS EC2 Key Pairs page. On the left, there's a sidebar with various navigation options like EC2 대시보드, 이벤트, 태그, 제한, 인스턴스, 이미지, Elastic Block Store, 네트워크 및 보안, 보안 그룹, 탐색적 IP, 배치 그룹, 키 페어 (which is underlined), 네트워크 인터페이스, 로드 밸런싱, and Auto Scaling. The main content area has a header '키 페어 (1)' and a search bar '키 페어 필터링'. Below it is a table with one row:

<input type="checkbox"/>	이름	지문	ID
<input type="checkbox"/>	builders20210312	07:ee:ad:fd:42:28:7f:32:48:02:16:37:2d:7d:0a...	key-0ec6d08580c0016dc

## 2. Cloudformation에서 생성.

AWS 관리 콘솔 - Cloudformation 으로 이동하고, 새로운 리소스를 선택 합니다.

다운로드 받은 파일 중에 IAD-VPC.yml, IAD-TGW.yml 을 사용합니다.

IAD-VPC 를 Cloudformation 을 기반으로 생성합니다.

CloudFormation > Stacks

Stacks (0)

No stacks

No stacks to display

Create stack

View getting started guide

Stack actions ▾ Create stack ▾

With new resources (standard)  
With existing resources (import resources)

다운로드 받아 둔 파일 중에서 IAD-VPC.yml 파일을 업로드하고, 다음을 선택합니다.

## 스택 생성

### 사전 조건 - 템플릿 준비

템플릿 준비

모든 스택은 템플릿을 기반으로 합니다. 템플릿은 JSON 또는 YAML 텍스트 파일로, 스택에 포함하려는 AWS 리소스에 대한 구성 정보가 들어 있습니다.

준비된 템플릿  샘플 템플릿 사용  Designer에서 템플릿 생성

### 템플릿 지정

템플릿은 스택의 리소스와 속성을 설명하는 JSON 또는 YAML 파일입니다.

템플릿 소스

템플릿을 선택하면 템플릿이 저장될 Amazon S3 URL이 생성됩니다.

Amazon S3 URL  템플릿 파일 업로드

템플릿 파일 업로드

파일 선택  IAD-VPC.yml

JSON 또는 YAML 형식 파일

S3 URL: <https://s3-external-1.amazonaws.com/cf-templates-12p302ou0sygq-us-east-1/2021069iL4-IAD-VPC.yml>

취소

다음을 선택하고, 아래와 같아 스택이름은 파일명과 동일하게 입력합니다.

IAD-VPC

## 스택 세부 정보 지정

### 스택 이름

스택 이름

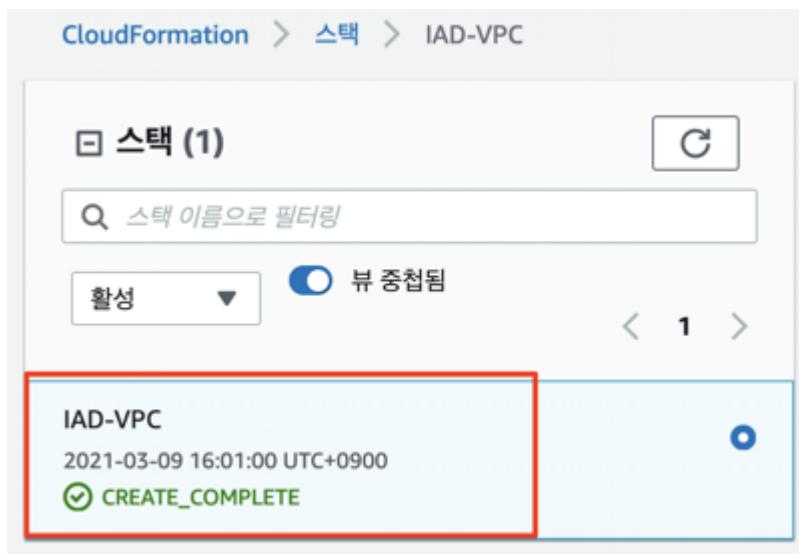
IAD-VPC

스택 이름은 문자(A-Z 및 a-z), 숫자(0-9) 및 대시(-)를 포함할 수 있습니다.

별도로 설정 변경없이, 다음 단계를 진행하고, 승인을 선택하고 스택생성합니다.



정상적으로 구성되면 아래와 같이 Cloudformation에서 확인 할 수 있습니다. VPC는 각 3분 내외에 생성됩니다.



## Task2. TGW구성하기.

IAD-VPC를 연결할 TransitGateway를 버지니아 리전(us-east-1)에 Cloudformation으로 생성합니다. 다운로드 받은 파일 중에, **IAD-TGW.yml** 파일을 업로드 합니다.

## 스택 생성

### 사전 조건 - 템플릿 준비

#### 템플릿 준비

모든 스택은 템플릿을 기반으로 합니다. 템플릿은 JSON 또는 YAML 텍스트 파일로, 스택에 포함하려는 AWS 리소스에 대한 구성 정보가 들어 있습니다.

준비된 템플릿

샘플 템플릿 사용

Designer에서 템플릿 생성

#### 템플릿 지정

템플릿은 스택의 리소스와 속성을 설명하는 JSON 또는 YAML 파일입니다.

#### 템플릿 소스

템플릿을 선택하면 템플릿이 저장될 Amazon S3 URL이 생성됩니다.

Amazon S3 URL

템플릿 파일 업로드

#### 템플릿 파일 업로드

파일 선택

IAD-TGW.yml

JSON 또는 YAML 형식 파일

S3 URL: <https://s3-external-1.amazonaws.com/cf-templates-12p302ou0syqq-us-east-1/2021069qJu-IAD-TGW.yml>

[Designer에서 보기](#)

다음을 선택하고, 아래와 같아 스택이름은 파일명과 동일하게 입력합니다. (TGW는 스택이름을 다르게 지정해도, 본 랙을 구성하는데 문제가 없습니다.)

## 스택 세부 정보 지정

### 스택 이름

#### 스택 이름

IAD-TGW

스택 이름은 문자(A-Z 및 a-z), 숫자(0-9) 및 대시(-)를 포함할 수 있습니다.

5분 이내에 TransitGateway가 완성됩니다.

## ▣ 스택 (2)



스택 이름으로 필터링

활성

뷰 중첩됨

< 1 >

IAD-TGW

2021-03-11 01:43:26 UTC+0900

CREATE\_COMPLETE



## Task3. VPC, EC2 구성 확인하기.

AWS 관리콘솔 - VPC 를 선택합니다.

VPC가 정상적으로 생성되었는지 확인합니다.

VPC (2) 정보					
<input type="text"/> VPC 필터링					
	Name	VPC ID	상태	IPv4 CIDR	IPv6 CIDR(네트워크 경계 그룹)
<input type="checkbox"/>	-	vpc-192a9d64	<input checked="" type="checkbox"/> Available	172.31.0.0/16	-
<input type="checkbox"/>	IAD-VPC	vpc-0115f15b3ebc4631f	<input checked="" type="checkbox"/> Available	10.5.0.0/16	-

AWS 관리콘솔 - EC2를 선택합니다.

EC2가 정상적으로 생성되었는지 확인합니다.

인스턴스 (2) 정보										
<input type="text"/> 인스턴스 필터링										
<input checked="" type="checkbox"/> 인스턴스 상태: running <input type="button" value="필터 지우기"/>										
	Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	피블릭 IPv4 DNS	피블릭 IPv4 주소	탄력적 IP
<input type="checkbox"/>	IAD-VPC-Public-1...	i-035c11cb024b274da	<input checked="" type="checkbox"/> 실행 중	t3.micro	<input checked="" type="checkbox"/> 2/2개 검사 통과	경보 없음	+	us-east-1a	ec2-44-192-97-166.compute...	44.192.97.166
<input type="checkbox"/>	IAD-VPC-Private-...	i-00587949de79e0ad4	<input checked="" type="checkbox"/> 실행 중	t3.micro	<input checked="" type="checkbox"/> 2/2개 검사 통과	경보 없음	+	us-east-1a	-	-

## Task 4. TGW 구성 확인

AWS 관리콘솔 - VPC - **TransitGateway** 를 선택해서, Transit Gateway 정상적으로 구성되었는지 확인합니다.

### ▼ TRANSIT GATEWAY

#### Transit Gateway

Transit Gateway 연결

Transit Gateway 라우팅 테이블

Transit Gateway 멀티캐스트

네트워크 관리자

Transit Gateway ID tgw-020596ddcb7c2da86			
Details		Tags	
Transit Gateway ID	tgw-020596ddcb7c2da86	Owner account ID	755764831759
State	available	Amazon ASN	65002
DNS support	enable	VPN ECMP support	enable
Auto accept shared attachments	enable	Default association route table	disable
Association route table ID	-	Default propagation route table	disable
Propagation route table ID	-	Multicast support	disable
Transit Gateway CIDR blocks	-		

## Task5. TGW Attachment 확인.

VPC-Transit Gateway-Transit Gateway 연결 을 선택해서, Transit Gateway attachment 가 정상적으로 구성되었는지 확인합니다.

Create Transit Gateway Attachment			
작업			
Transit Gateway attachment ID tgw-attach-08241f40f91b73c9b			
Transit Gateway attachment ID tgw-attach-08241f40f91b73c9b			
Transit Gateway attachment ID	tgw-attach-08241f40f91b73c9b	Transit Gateway owner ID	755764831759
Transit Gateway ID	tgw-020596ddcb7c2da86	Resource owner account ID	755764831759
Resource type	VPC	State	available
Resource ID	vpc-0115f15b3ebc4631f	Associated route table ID	tgw-rtb-06f42b6f6c10ecded
Association state	associated	Association state	associated
IPv6 support	disable	Subnet IDs	subnet-03b9e7479adcc15d8

IAD-TGW-Attach-IAD-VPC를 선택하면, 이미 "IAD-VPC"의 TGW-Subnet ID에 연결되어 있는 것을 확인할 수 있습니다. 또한 Routing Table에 Association 된 상태도 확인이 가능합니다.

1. TGW Routing Table과 Attachment가 연결된 상태를 확인
2. Attachment가 VPC의 어떤 Subnet과 연결되었는지 확인

## Task6. TGW Routing Table 확인.

VPC-Transit Gateway-Transit Gateway- Transit Gateway 라우팅 테이블을 선택해서 라우팅 테이블 구성을 확인해 봅니다. Associations와 Propagation 탭을 눌러서, IAD-VPC 연결과 IAD-VPC의 CIDR가 정상적으로 업데이트 되었는지 확인합니다.

The screenshot shows two screenshots of the AWS CloudFormation console. The top screenshot displays the 'Associations' tab for a Transit Gateway Route Table named 'tgw-rtb-06f42b6f6c10ecded'. It lists one association with an Attachment ID of 'tgw-attach-08241f40f91b73c9b', a Resource type of 'VPC', a Resource ID of 'vpc-0115f15b3ebc4631f', and a State of 'associated'. The bottom screenshot shows the 'Propagations' tab for the same Transit Gateway Route Table. It lists one propagation with an Attachment ID of 'tgw-attach-08241f40f91b73c9b', a Resource type of 'VPC', a Resource ID of 'vpc-0115f15b3ebc4631f', and a State of 'enabled'.

propagation이 정상적으로 구성되었기 때문에 Route 탭을 선택하면, Route Type은 Propagated 되었다고 표기됩니다.

Details	Associations	Propagations	Prefix list references	Routes	Tags
The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.					
Create static route		Replace static route		Delete static route	
<input type="text"/> 속성별 필터 또는 키워드별 검색					
<input type="checkbox"/> CIDR	Attachment		Resource type	Route type	Route state
<input type="checkbox"/> 10.5.0.0/16	tgw-attach-08241f40f91b73c9b   vpc-0115f15b3ebc4631f		VPC	propagated	active

Cloudformation을 통해서 모두 정상적으로 구성되었습니다. 🙌

### 3. TGW Peering 구성

#### Task7. SSM에서 인스턴스 확인

모든 랩의 구성 시험은 Private 인스턴스로 시험합니다. Cloudformation을 통해 System Manager와 Session Manager를 사용할 수 있도록 자동 배포 구성하였습니다.

Session Manager를 사용할 수 있도록 아래 같이 각 PC환경에 맞추어서 AWS Session Manager Plugin을 설치합니다. Cloud9을 사용하거나 웹콘솔에서 Session Manager를 사용하면 각 PC환경에서 설치할 필요가 없습니다.

Cloud9 터미널에서 아래 aws cli 명령을 실행하여 생성된 us-east-1의 EC2 인스턴스를 확인합니다.

```
1 aws ec2 describe-instances --query 'Reservations[].Instances[].[Tags[?Key=
```

실행한 예제입니다.

```
1 whchoi:~/environment $ aws ec2 describe-instances --query 'Reservations[.]'
2 -----
3 |
4 +-----+-----+-----+
5 | IAD-VPC-Public-10.5.11.101 | us-east-1a | i-035c11cb024b274da | t3.m
6 | IAD-VPC-Private-10.5.21.101| us-east-1a | i-00587949de79e0ad4 | t3.m
```

ssm plugin을 통해서 인스턴스 ID 기반으로, 직접 Private Instance에 접속합니다. 아래와 같은 명령을 통해서 직접 Private Instance에 접속합니다.

- **IAD-VPC-Private-10.5.21.101**

```
1 aws ssm start-session --target "IAD-VPC-Private-10.5.21.101" --region us-e
2
```

Cloud9에서 터미널 창을 1개를 추가로 오픈하고, 아래와 같이 각 6개의 호스트에 명령을 입력하여, bash 콘솔로 접속하고, 시험할 호스트들을 host file에 등록합니다.

```
1 sudo -s
2 echo 10.0.21.101 SEOUL-VPC-HQ-Private >> /etc/hosts
3 echo 10.1.21.101 SEOUL-VPC-PRD-Private >> /etc/hosts
4 echo 10.2.21.101 SEOUL-VPC-STG-Private >> /etc/hosts
5 echo 10.3.21.101 SEOUL-VPC-DEV-Private >> /etc/hosts
6 echo 10.4.21.101 SEOUL-VPC-PRT-Private >> /etc/hosts
7 echo 10.5.21.101 IAD-VPC-Private >> /etc/hosts
8
```

## Task8. 시나리오 이해하기

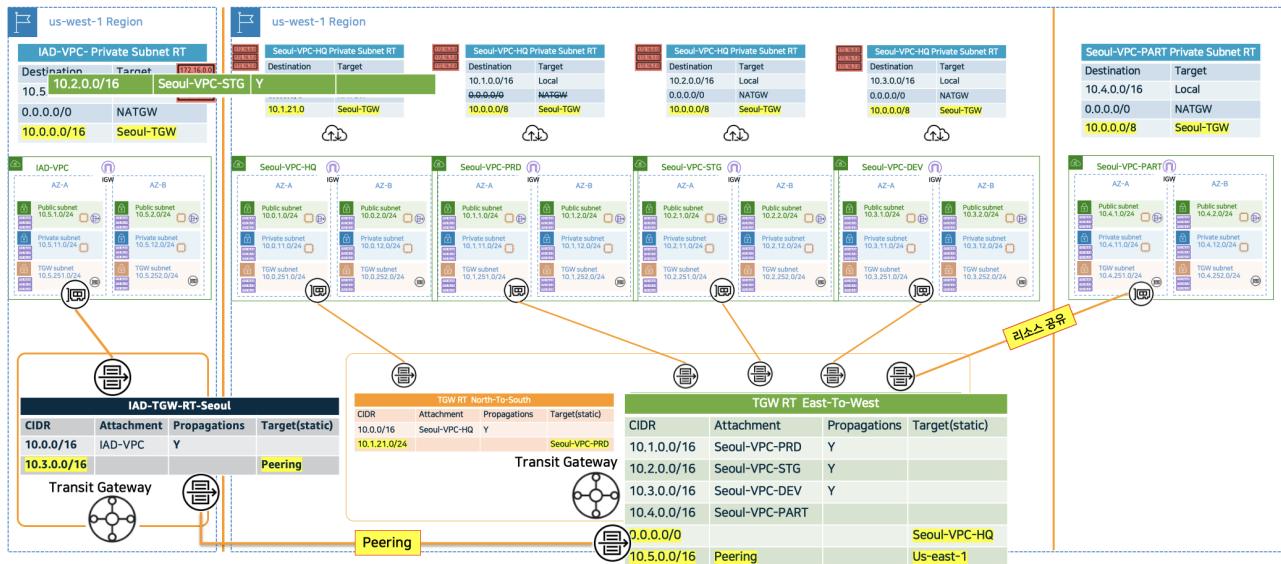
1. 빌더스 컴퍼니는 아래와 같은 VPC를 2개의 리전에 소유하고 있습니다.

- IT Control Tower : Seoul-VPC-HQ
- Production Workload : Seoul-VPC-PRD
- Staging Workload : Seoul-VPC-STG
- Dev Workload : Seoul-VPC-Dev
- Dev Workload: IAD-VPC

2. 미국의 개발인력들이 한국의 개발 인력들 (Seoul-VPC-DEV) 간의 잦은 네트워크 연결이 필요합니다.

### 3. 미국의 개발인력들은 한국의 리전의 인터넷을 사용하지는 않을 것입니다.

목표 구성과 필요작업은 아래와 같습니다.



### Task9. 버지니아 리전과 한국 리전 연결 (Peering)

AWS 관리콘솔 - VPC - Transit Gateway - Transit Gateway 연결 을 선택합니다.

Create Transit Gateway Attachment 를 선택합니다.

## Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

1 **Transit Gateway ID\*** tgw-020596ddcb7c2da86  

2 **Attachment type** Peering Connection  

### Peering Connection Attachment

Select and configure your peering connection attachment.

3 **Attachment name tag** IAD-TO-SEOUL 

Account  My account  Other account

4 **Region** Seoul (ap-northeast-2)  

5 **Transit gateway (accepter)\*** tgw-0c4098960edd00ae6 

1. Transit Gateway ID - 버지니아에서 생성한 IAD-TGW를 선택합니다.

2. Attachment Type - Peering Connection 을 선택 합니다. (주의 !!!)

3. Attachment name tag - 연결 이름을 입력합니다.

IAD-TO-SEOUL

4. Region - Seoul(ap-northeast-2)를 선택합니다. (원격지 리전을 의미합니다.)

5. Transit Gateway(accepter) - 원격지 서울 리전에 만들어져 있는 Transit Gateway ID를 입력합니다.

미리 열어둔 브라우저의 서울리전 탭에, AWS 관리콘솔 좌측 상단에서 ap-northeast-2 (서울 리전)을 선택합니다.

AWS 관리 콘솔 - VPC - Transit Gateway - Transit Gateway 를 선택하고, Transit Gateway ID를 복사합니다.

The screenshot shows the AWS Management Console with the search bar set to '서비스, 기능, 마켓플레이스 제품, 설명서 검색 [Option+S]'. The user is in the '서울' region. The 'Create Transit Gateway' button is visible. A table lists existing Transit Gateways, with 'Seoul-TGW' selected and its ID 'tgw-0c4098960edd00ae6' highlighted. The 'Details' tab is selected, showing the Transit Gateway ID, State (available), DNS support (enable), Auto accept shared attachments (enable), Association route table ID (-), Propagation route table ID (-), Owner account ID (755764831759), Amazon ASN (65001), VPN ECMP support (enable), Default association route table (disable), Default propagation route table (disable), and Multicast support (disable).

이제 5번의 Transit Gateway (accepter)에 서울 리전의 Transit Gateway ID값을 붙여 넣고, Create Attachment를 클릭하고 완료합니다. 아래와 같이 새로운 Transit Gateway Attachment가 생성되었습니다.

The screenshot shows the 'Create Transit Gateway Attachment' page. A table lists existing attachments, with 'IAD-TO-SEOUL' selected and its state highlighted as 'initiating request'. The 'Details' tab is selected, showing Requester owner ID (755764831759), Requester transit gateway ID (tgw-020596ddcb7c2da86), Requester region (N. Virginia (us-east-1)), Transit Gateway attachment ID (tgw-attach-04c969b75b8a1779a), Resource type (Peering), Acceptor owner ID (755764831759), Acceptor Transit Gateway ID (tgw-0c4098960edd00ae6), Acceptor region (Seoul (ap-northeast-2)), State (initiating request), and Associated route table (-).

하지만 서울리전 Transit Gateway Peering을 위한 Transit Gateway Attachment는 initiating request 상태입니다. 서울리전에서 수락하지 않으면 연결되지 않습니다.

이제 다시 서울리전의 콘솔 창이 열려있는 브라우저 탭을 선택합니다.

서울 리전의 VPC - Transit Gateway - Transit Gateway 연결 에 새로운 Transit Gateway Attachment가 생성된 것을 확인 할 수 있습니다. 하지만 pending acceptance 상태입니다.

Create Transit Gateway Attachment 작업 ▾

Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State	Associated route table ID	Association
<input checked="" type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-PRD	tgw-attach-04ce9ef45b52dec1	tgw-0c4098960edd00ae6	Peering	vpc-0624a2ec3218da430	pending acceptance	-	-
<input type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-STG	tgw-attach-088f2f44c578cecb1	tgw-0c4098960edd00ae6	VPC	vpc-0d033093356d0c91f	available	tgw-rb-08c85e2b1cedd08b4	associated
<input type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-HQ	tgw-attach-09f64c384fcbeff084	tgw-0c4098960edd00ae6	VPC	vpc-042f10f02be8c68f0	available	tgw-rb-017613c25a76e4e88	associated
<input type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-DEV	tgw-attach-0fa29ce7ade483dbc	tgw-0c4098960edd00ae6	VPC	vpc-0fb6ca7e9cd6df048	available	tgw-rb-08c85e2b1cedd08b4	associated

Transit Gateway Attachment: tgw-attach-04c969b75b8a1779a

Details Tags

Requester owner ID: 755764831759  
 Requester transit gateway ID: tgw-020596ddcb7c2da86  
 Requester region: N. Virginia (us-east-1) **요청한 리전**  
 Transit Gateway attachment ID: tgw-attach-04c969b75b8a1779a  
 Resource type: Peering  
 Association state: -

Acceptor owner ID: 755764831759  
 Acceptor Transit Gateway ID: tgw-0c4098960edd00ae6  
 Acceptor region: Seoul (ap-northeast-2)  
 State: pending acceptance **수락 대기 중...**  
 Associated route table: -

상단 "작업" 을 선택하고 **Accept** 선택합니다.

Create Transit Gateway Attachment 작업 ▾

Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State	Associated route table ID
<input checked="" type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-PRD	tgw-attach-04ce9ef45b52dec1	tgw-0c4098960edd00ae6	Peering	vpc-0624a2ec3218da430	available	tgw-rb-08c85e2b1cedd08b4
<input type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-STG	tgw-attach-088f2f44c578cecb1	tgw-0c4098960edd00ae6	VPC	vpc-0d033093356d0c91f	available	tgw-rb-08c85e2b1cedd08b4
<input type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-HQ	tgw-attach-09f64c384fcbeff084	tgw-0c4098960edd00ae6	VPC	vpc-042f10f02be8c68f0	available	tgw-rb-017613c25a76e4e88
<input type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-DEV	tgw-attach-0fa29ce7ade483dbc	tgw-0c4098960edd00ae6	VPC	vpc-0fb6ca7e9cd6df048	available	tgw-rb-08c85e2b1cedd08b4

수락 선택

Accept를 선택하면, pending 으로 전환되고 7~8분 이후 available로 변경됩니다.



Create Transit Gateway Attachment 작업 ▾

Attachment Tag name을 변경해 드립니다.

Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State
<input checked="" type="checkbox"/> Seoul-To-Virginia	tgw-attach-04c969b75b8a1779a	tgw-0c4098960edd00ae6	Peering	tgw-020596ddcb7c2da86	pending
<input type="checkbox"/> 17/255	tgw-attach-04ce9ef45b52dec1	tgw-0c4098960edd00ae6	VPC	vpc-0624a2ec3218da430	available
<input type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-STG	tgw-attach-088f2f44c578cecb1	tgw-0c4098960edd00ae6	VPC	vpc-0d033093356d0c91f	available
<input type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-HQ	tgw-attach-09f64c384fcbeff084	tgw-0c4098960edd00ae6	VPC	vpc-042f10f02be8c68f0	available
<input type="checkbox"/> Seoul-TGW-Attach-Seoul-VPC-DEV	tgw-attach-0fa29ce7ade483dbc	tgw-0c4098960edd00ae6	VPC	vpc-0fb6ca7e9cd6df048	available

이제 Attachment가 Association으로 변경되면, Transit Gateway-Transit Gateway Route Table 탭에서 Create Association 을 시켜 줍니다.

## Create association

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated to one route table.

Transit Gateway ID tgw-0c4098960edd00ae6

Transit Gateway route table ID tgw-rb-08c85e2b1cedd08b4

Choose attachment to associate\*

C Attachment된 peer를 Association 시켜 줍니다.

* 필수 사항	Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Association route table
	tgw-attach-04c969b75b8a1779a	Seoul-To-Virginia	tgw-020596ddcb7c2da86	peering	755764831759	tgw-rb-08c85e2b1cedd08b4
	tgw-attach-04cea9ef45b52dec1	Seoul-TGW-Attach-Seoul-VPC-PRD	vpc-0624a2ec3218da430	vpc	755764831759	tgw-rb-08c85e2b1cedd08b4
	tgw-attach-088f2f44c578cecb1	Seoul-TGW-Attach-Seoul-VPC-STG	vpc-0d033093356d0c91f	vpc	755764831759	tgw-rb-08c85e2b1cedd08b4
	tgw-attach-09f64c384fcbe084	Seoul-TGW-Attach-Seoul-VPC-HQ	vpc-042f10f02be8c68f0	vpc	755764831759	tgw-rb-017613c25a76e4e88
	tgw-attach-0fa29ce7ade483dbc	Seoul-TGW-Attach-Seoul-VPC-DEV	vpc-0fb6ca7e9cd6df048	vpc	755764831759	tgw-rb-08c85e2b1cedd08b4

Create Transit Gateway Route Table 작업 ▾

Tags 및 속성별 필터 또는 키워드별 검색

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
<input checked="" type="checkbox"/> Seoul-TGW-RT-East-To-West	tgw-rb-08c85e2b1cedd08b4	tgw-0c4098960edd00ae6	available	No	No
<input type="checkbox"/> Seoul-TGW-RT-North-To-South	tgw-rb-017613c25a76e4e88	tgw-0c4098960edd00ae6	available	No	No

Transit Gateway Route Table: tgw-rb-08c85e2b1cedd08b4

Details Associations Propagations Prefix list references Routes Tags

Create association Delete association

Peering 이 Association에 추가 되었습니다.

Attachment ID	Resource type	Resource ID	State
<input type="checkbox"/> tgw-attach-0fa29ce7ade483dbc	VPC	vpc-0fb6ca7e9cd6df048	associated
<input checked="" type="checkbox"/> tgw-attach-04c969b75b8a1779a	Peering	tgw-0c4098960edd00ae6	associated
<input type="checkbox"/> tgw-attach-04cea9ef45b52dec1	VPC	vpc-0624a2ec3218da430	associated
<input type="checkbox"/> tgw-attach-088f2f44c578cecb1	VPC	vpc-0d033093356d0c91f	associated

이제 다시 버지니아 리전 콘솔로 이동합니다.

AWS 콘솔 - VPC - Transit Gateway - Transit Gateway 라우팅 테이블을 선택하고, Create association을 선택합니다.

New VPC Experience Tell us what you think

VPC 대시보드 New

VPC로 필터링:

VPC 선택

- ▶ 가상 프라이빗 라우트
- ▶ 보안
- ▶ REACHABILITY
- ▶ AWS 네트워크 방화벽
- ▶ VPN(가상 프라이빗 네트워크)
- ▼ TRANSIT GATEWAY
- Transit Gateway
- Transit Gateway 연결
- Transit Gateway 라우팅 테이블
- Transit Gateway 멀티캐스트 네트워크 관리자

Create Transit Gateway Route Table 작업 ▾

Tags 및 속성별 필터 또는 키워드별 검색

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
<input checked="" type="checkbox"/> IAD-TGW-RT-Seoul	tgw-rb-06f42b6f6c10ecd6	tgw-020596ddcb7c2da86	available	No	No

Transit Gateway Route Table: tgw-rb-06f42b6f6c10ecd6

Details Associations Propagations Prefix list references Routes Tags

Create association Delete association

속성별 필터 또는 키워드별 검색

Attachment ID	Resource type	Resource ID	State
<input type="checkbox"/> tgw-attach-08241f40f91b73c9b	VPC	vpc-0115f15b3ebc4631f	associated

새로운 peering을 Association 시켜 줍니다.

Transit Gateway Route Tables > Create association

### Create association

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated to one route table.

Transit Gateway ID tgw-020596ddcb7c2da86

Transit Gateway route table ID tgw-rtb-06f42b6f6c10ecded

Choose attachment to associate\*

새로운 peering 을 Association 시켜 줍니다.

\* 필수 사항

Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Association route table
tgw-attach-04c969b75b8a1779a	IAD-TO-SEOUL	tgw-0c4098960edd00ae6	peering	755764831759	
tgw-attach-08241f40f91b73c9b	IAD-TGW-Attach-IAD-VPC	vpc-0115f15b3ebc4631f	vpc	755764831759	tgw-rtb-06f42b6f6c10ecded

New VPC Experience Tell us what you think

VPC 대시보드 New

VPC로 필터링: VPC 선택

▶ 가상 프라이빗 클라우드

▶ 보안

▶ REACHABILITY

▶ AWS 네트워크 방화벽

▶ VPN(기상 프라이빗 네트워크)

▼ TRANSIT GATEWAY

Transit Gateway

Transit Gateway 연결

Transit Gateway 라우팅 테이블

Create Transit Gateway Route Table 작업

태그 및 속성별 필터 또는 키워드별 검색

Name Transit Gateway route table ID State Default association route table Default propagation route table

IAD-TGW-RT-Seoul tgw-rtb-06f42b6f6c10ecded tgw-020596ddcb7c2da86 available No No

Transit Gateway Route Table: tgw-rtb-06f42b6f6c10ecded

Details Associations Propagations Prefix list references Routes Tags

Create association Delete association

속성별 필터 또는 키워드별 검색 Peering or Association에 추가 되었습니다.

Attachment ID	Resource type	Resource ID	State
tgw-attach-08241f40f91b73c9b	VPC	vpc-0115f15b3ebc4631f	associated
tgw-attach-04c969b75b8a1779a	Peering	tgw-020596ddcb7c2da86	associated

## Task10. Transit Gateway 라우팅 테이블 변경

Peering은 구성을 완료했지만, 상호간의 라우팅 구성이 되어 있지 않았습니다.

먼저 서울리전에서 버지니아 리전으로 라우팅을 구성해 줍니다.

서울 리전 관리콘솔이 열려있는 브라우저 탭을 선택하고, AWS 관리콘솔 - VPC - Transit Gateway - Transit Gateway 라우팅 테이블을 선택합니다.

Seoul-TGW-RT-East-To-West 를 선택하고, Route 탭을 선택하고, Create static Route를 선택합니다.

New VPC Experience  
Tell us what you think

VPC 대시보드 New

VPC로 필터링:

▶ 가상 프라이빗 클라우드

▶ 보안

▶ REACHABILITY

▶ VPN(가상 프라이빗 네트워크)

▼ TRANSIT GATEWAY

- Transit Gateway
- Transit Gateway 연결
- Transit Gateway 미우팅 테이블**
- Transit Gateway 멀티캐스트
- 네트워크 관리자
- ▼ 트래픽 미러링
- 미리 세션 New

Create Transit Gateway Route Table 작업 ▾

태그 및 속성별 필터 또는 키워드별 검색

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
Seoul-TGW-RT-East-To-West	tgw-rb-08c85e2b1cedd08b4	tgw-0c4098960edd00ae6	available	No	No
Seoul-TGW-RT-North-To-South	tgw-rb-017613c25a76e4e88	tgw-0c4098960edd00ae6	available	No	No

Transit Gateway Route Table: tgw-rb-08c85e2b1cedd08b4

Details Associations Propagations Prefix list references Routes Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create static route Replace static route Delete static route

속성별 필터 또는 키워드별 검색

CIDR	Attachment	Resource type	Route type	Route state	Prefix List ID
10.1.0.0/16	tgw-attach-04cea9ef45b52dec1   vpc-0624a2ec3218da430	VPC	propagated	active	-
10.2.0.0/16	tgw-attach-088f2f44c578cecb1   vpc-0d033093356dc91f	VPC	propagated	active	-
10.3.0.0/16	tgw-attach-0fa29ce7ade483dbc   vpc-0fb6ca7e9cd6df048	VPC	propagated	active	-

CIDR 주소를 버지니아 리전에 생성한 VPC CIDR 주소를 입력합니다.

10.5.0.0/16

Choose attachment는 Seoul-To-Virginia를 선택합니다.

Transit Gateway Route Tables > Create static route

### Create static route

Add a static route to your Transit Gateway route table.

Transit Gateway ID tgw-0c4098960edd00ae6

Transit Gateway route table ID tgw-rb-08c85e2b1cedd08b4

CIDR\*  ⓘ 베지니아 리전(us-east-1)의 CIDR 주소가 목적지

Blackhole  ⓘ

Choose attachment

Seoul-To-Virginia 선택

속성별 필터

Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Association route table
tgw-attach-04c969b75bb8a1779a	Seoul-To-Virginia	tgw-020596ddcb7c2da86	peering	755764831759	tgw-rb-08c85e2b1cedd08b4
tgw-attach-04cea9ef45b52dec1	Seoul-TGW-Attach-Seoul-VPC-PRD	vpc-0624a2ec3218da430	vpc	755764831759	tgw-rb-08c85e2b1cedd08b4
tgw-attach-088f2f44c578cecb1	Seoul-TGW-Attach-Seoul-VPC-STG	vpc-0d033093356dc91f	vpc	755764831759	tgw-rb-08c85e2b1cedd08b4
tgw-attach-09f64c384fcbeff084	Seoul-TGW-Attach-Seoul-VPC-HQ	vpc-042110f02be8c68f0	vpc	755764831759	tgw-rb-017613c25a76e4e88
tgw-attach-0fa29ce7ade483dbc	Seoul-TGW-Attach-Seoul-VPC-DEV	vpc-0fb6ca7e9cd6df048	vpc	755764831759	tgw-rb-08c85e2b1cedd08b4

아래와 같이 새롭게 라우팅 테이블이 추가 되었습니다.

Transit Gateway Route Table: tgw-rtb-08c85e2b1cedd08b4

CIDR	Attachment	Resource type	Route type	Route state	Prefix List ID
10.1.0.0/16	tgw-attach-04cea9ef45b52dec1   vpc-0624a2ec3218da430	VPC	propagated	active	-
10.2.0.0/16	tgw-attach-088f2f44c578cecb1   vpc-0d033093356d0c91f	VPC	propagated	active	-
10.3.0.0/16	tgw-attach-0fa29ce7ade483dbc   vpc-0fb6ca7e9cd6df048	VPC	propagated	active	-
10.5.0.0/16	tgw-attach-04c969b75b8a1779a   tgw-020596ddcb7c2da86	Peering	static	active	-

이제 버지니아 리전에서 서울로 오는 경로만 설정하면 됩니다. 버지니아 리전의 콘솔 창이 열려 있는 브라우저 탭을 선택합니다.

**AWS 관리 콘솔 - VPC - Transit Gateway - Transit Gateway 라우팅 테이블 - IAD-TGW-RT-Seoul - Route 탭- Create static Route 선택**

합니다.

Create Transit Gateway Route Table

Name: IAD-TGW-RT-Seoul

Transit Gateway route table ID: tgw-rtb-06f42b6f6c10ecded

Destination CIDR: 10.5.0.0/16

Attachment: tgw-020596ddcb7c2da86

Create static route

CIDR 주소를 서울리전의 Seoul-VPC-DEV CIDR 주소를 입력합니다.

10.3.0.0/16

Choose attachment은 IAD-TO-SEOUL 선택하고, Create Static Route를 선택합니다.

## Create static route

Add a static route to your Transit Gateway route table.

Transit Gateway ID tgw-020596ddcb7c2da86

Transit Gateway route table ID tgw-rtb-06f42b6f6c10ecded

CIDR\*

Blackhole   ⓘ

Seoul-VPC-DEV CIDR 주소

Choose attachment \* 필수 사항

IAD-TO-SEOUL 선택

Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Association route table
tgw-attach-04c969b75b8a1779a	IAD-TO-SEOUL	tgw-0c4098960edd00ae6	peering	755764831759	tgw-rtb-06f42b6f6c10ecded
tgw-attach-08241f40f91b73c9b	IAD-TGW-Attach-IAD-VPC	vpc-0115f15b3ebc4631f	vpc	755764831759	

아래와 같이 새롭게 라우팅 테이블이 추가 되었습니다.

**Create Transit Gateway Route Table** 작업 ▾

태그 및 속성별 필터 또는 키워드별 검색

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
IAD-TGW-RT-Seoul	tgw-rtb-06f42b6f6c10ecded	tgw-020596ddcb7c2da86	available	No	No

Transit Gateway Route Table: tgw-rtb-06f42b6f6c10ecded

Details Associations Propagations Prefix list references Routes Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

**Create static route** Replace static route Delete static route

속성별 필터 또는 키워드별 검색

CIDR	Attachment	새롭게 추가된 라우팅 테이블	Resource type	Route type	Route state	Prefix List ID
10.3.0.0/16	tgw-attach-04c969b75b8a1779a   tgw-0c4098960edd00ae6	Peering	static	active	-	-
10.5.0.0/16	tgw-attach-08241f40f91b73c9b   vpc-0115f15b3ebc4631f	VPC	propagated	active	-	-

이제 버지니아 리전의 IAD-VPC-Private-Subnet-A-RT 라우팅 테이블에서 Seoul-VPC-DEV 의 CIDR 주소에 대한 라우팅 테이블만 편집하면 됩니다.

AWS 관리 콘솔 - VPC - 가상 프라이빗 클라우드 - 라우팅 테이블 - IAD-VPC-Private=Subnet-A-RT 선택

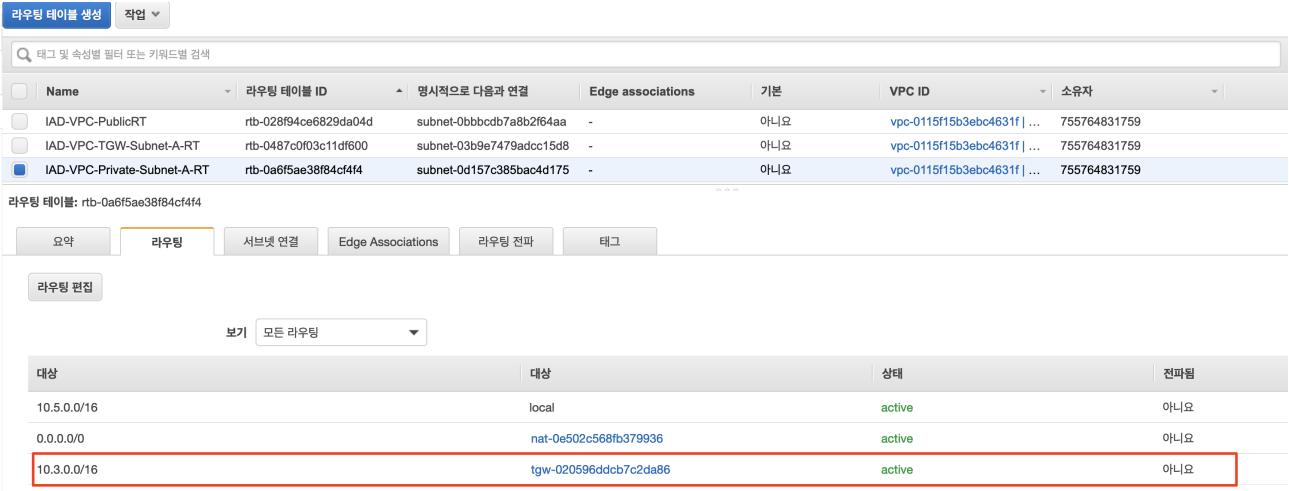
라우팅 편집을 선택하고, Seoul-VPC-DEV CIDR 주소에 대한 라우팅 테이블을 구성합니다.

10.3.0.0/16

## 라우팅 편집

대상	대상	상태	전파됨
10.5.0.0/16	local	active	아니요
0.0.0.0/0	nat-0e502c568fb379936	active	아니요
10.3.0.0/16	tgw-020596ddcb7c2da86	active	아니요

10.3.0.0/16 CIDR 주소가 Transit Gateway 로 향하도록 추가합니다.



The screenshot shows the AWS Cloud9 terminal interface. The user has run the command `ping SEOUL-VPC-DEV-Private`. The output shows the ping request being sent to the private IP address 10.3.21.101. The response indicates that the connection is successful, with a round-trip time of approximately 1 ms.

```
ping SEOUL-VPC-DEV-Private
PING 10.3.21.101(10.3.21.101) 56(84) bytes from 10.5.21.101: icmp_seq=1 ttl=64 time=1.04 ms

```

## Task 11. 트래픽 전송 확인

이제 Cloud9 콘솔 터미널 IAD-VPC-Private 10.5.21.101에서 정상적으로 Seoul-VPC-DEV 10.3.21.101로 ping이 이뤄지는지 확인합니다.

```
ping SEOUL-VPC-DEV-Private
```

다른 서울 리전 EC2 트래픽 전송이 되는지 확인합니다. 다른 EC2 인스턴스들로는 연결되지 않아야 합니다.

- 1 ping SEOUL-VPC-PRD-Private
- 2 ping SEOUL-VPC-STG-Private
- 3 ping SEOUL-VPC-HQ-Private



서로 다리전에서 TGW 연동을 확인해 보았습니다. Propagation과 Static 조합을 통해서 VPC 격리와 보안을 강화하는 여러가지 디자인을 구성해 볼 수 있습니다.

해당 LAB의 질문 사항은 [whchoi98@gmail.com](mailto:whchoi98@gmail.com) / [whchoi@amazon.com](mailto:whchoi@amazon.com) 또는 **슬랙채널** (<https://whchoi-hol.slack.com/archives/C01QM79Q4BD>)에서 문의 가능합니다.

# Transit Gateway Monitoring

## 1. 네트워크 매니저 소개

Transit Gateway Network Manager(Network Manager)를 사용하면 전송 게이트웨이를 중심으로 구축된 네트워크를 중앙에서 관리할 수 있습니다. AWS 리전 및 온프레미스 위치에서 글로벌 네트워크를 시각화하고 모니터링할 수 있습니다.

- **글로벌 네트워크** – 네트워크 객체의 상위 수준 컨테이너 역할을 하는 단일 프라이빗 네트워크입니다.
- **디바이스** – 온프레미스 네트워크, 데이터 센터, AWS 클라우드 또는 기타 클라우드 공급자의 물리적 또는 가상 어플라이언스를 나타냅니다.
- **연결** – 두 디바이스 간의 연결을 나타냅니다. 물리적 또는 가상 어플라이언스와 VPC 내 타사 가상 어플라이언스 간의 연결이거나 온프레미스 네트워크의 물리적 어플라이언스 간의 연결일 수 있습니다.
- **링크** – 사이트로부터의 단일 인터넷 연결을 나타냅니다.
- **사이트** – 물리적 온프레미스 위치를 나타냅니다. 지점, 사무실, 매장, 캠퍼스 또는 데이터 센터가 될 수 있습니다.

---

## 2. 네트워크 매니저 구성

Task1. 네트워크 매니저 생성

VPC - Transit Gateway - 네트워크 관리자 를 선택하고, Create a Global Network 를 선택합니다.

New VPC Experience  
Tell us what you think

VPC 대시보드 New

VPC로 필터링:  
 VPC 선택

▶ 가상 프라이빗 클라우드

▶ 보안

▶ REACHABILITY

▶ VPN(가상 프라이빗 네트워크)

▼ TRANSIT GATEWAY

- Transit Gateway
- Transit Gateway 연결
- Transit Gateway 라우팅 테이블
- Transit Gateway 멀티캐스트

**네트워크 관리자**

▼ 트래픽 미러링

- 미러 세션 New
- 미러 대상 New
- 미러 필터 New

Settings New

## Welcome to Network Manager



AWS Transit Gateway Network Manager lets you centrally manage your network across AWS and on-premise sites. Visualize your global network in a centralized dashboard, as a logical diagram or a geographic map. Monitor your network using CloudWatch metrics and events for changes in network topology, routing, and connection status.

[Learn more about Network Manager](#)

[View my Global Networks](#) [Create a Global Network](#)

글로벌 네트워크 생성에서 아래 내용을 설정하고, 글로벌 네트워크를 생성합니다.

- 이름 - 글로벌 네트워크 식별을 위한 이름을 정의합니다.

MyNetwork

## 글로벌 네트워크 생성

AWS 및 온프레미스 리소스를 포함하는 네트워크를 나타내는 글로벌 네트워크를 생성합니다. [자세히 알아보기](#)

**글로벌 네트워크 설정**

**이름**  
글로벌 네트워크를 식별하는 데 도움이 되는 이름입니다.

이름은 100자를 초과할 수 없습니다. 사용 가능한 문자는 a~z, 0~9, -(하이픈)입니다.

**설명**  
글로벌 네트워크를 식별하는 데 도움이 되는 설명입니다.

▶ 추가 설정

**Cancel** **글로벌 네트워크 생성**

정상적으로 생성되었는지 확인하고, 생성된 글로벌 네트워크를 선택 합니다.

⌚ 글로벌 네트워크를 생성했습니다.
Network Manager > 글로벌 네트워크

글로벌 네트워크 (1 of 4)

ID	이름	상태
<input checked="" type="checkbox"/> global-network-04117c16e7893f86d	MyNetwork	<span>Available</span>

전송 게이트웨이 등록을 선택합니다.

Network Manager > 글로벌 네트워크 > MyNetwork

개요 | 세부 정보 | 지리적 | 토플로지 | 이벤트 | 모니터링 | 경로 분석기

**MyNetwork 인벤토리**  
글로벌 네트워크의 일부인 네트워크 리소스입니다.

전송 게이트웨이	사이트	디바이스
0	0	0

**전송 게이트웨이 VPN 상태**

ID	이름	지역	VPN 종단	손상된 VPN	VPN 가동
전송 게이트웨이 없음 표시할 전송 게이트웨이가 없습니다. <b>전송 게이트웨이 등록</b>					

**전송 게이트웨이 Connect 피어 상태**

ID	이름	지역	Connect 피어 종단	Connect 피어가 손상됨	Connect 피어 가동
전송 게이트웨이 없음 표시할 전송 게이트웨이가 없습니다.					

앞서 만들어 둔 TransitGateway를 선택하고, 전송게이트웨이 등록을 클릭합니다.

Network Manager > 글로벌 네트워크 > MyNetwork > 전송 게이트웨이 > 등록

전송 게이트웨이 등록

이 글로벌 네트워크를 통해 시작화면과 모니터링할 전송 게이트웨이를 선택하고 등록합니다. 모든 AWS 리전에서 전송 게이트웨이를 선택할 수 있습니다. 각 전송 게이트웨이는 하나의 글로벌 네트워크에만 등록할 수 있습니다. 자세히 알아보기 [\[ \]](#)

**등록할 전송 게이트웨이 선택 (2 of 4)**

ID	이름	지역	상태
<input checked="" type="checkbox"/> tgw-0408d8883c27453ea	Seoul-TGW	ap-northeast-2	<b>Available</b>
<input type="checkbox"/> tgw-0427a4e5e96fc0bf2		ap-northeast-2	Available
<input checked="" type="checkbox"/> tgw-07e03d3bf6f418c4	IAD-TGW	us-east-1	Available
<input type="checkbox"/> tgw-0cba52098d724ea7b		us-west-1	Available

**전송 게이트웨이 등록**

전송 게이트웨이가 정상적으로 등록되었는지 확인합니다.

Network Manager > 글로벌 네트워크 > global-network-04117c16e7893fb6d > 전송 게이트웨이

전송 게이트웨이 (2)

ID	이름	지역	상태
<input type="checkbox"/> tgw-0408d8883c27453ea	Seoul-TGW	ap-northeast-2	Available
<input type="checkbox"/> tgw-07e03d3bf6f418c4	IAD-TGW	us-east-1	Available

Network Manager 좌측 대시보드의 대시보드 메뉴를 선택하고, 전송게이트웨이가 2개 등록 되었는지 확인합니다. 또한 전송게이트웨이의 Connection 상태를 확인합니다.

Network Manager > 글로벌 네트워크 > MyNetwork

개요 세부 정보 지리적 토플로지 이벤트 모니터링 경로 분석기

**MyNetwork**

Transit Gateways  
Devices  
Sites

**MyNetwork 인벤토리**  
글로벌 네트워크의 일부인 네트워크 리소스입니다.

전송 게이트웨이 2  
전송 게이트웨이 0  
사이트 0  
디바이스 0

**전송 게이트웨이 VPN 상태 (2)**

ID	이름	지역	VPN 중단	손상된 VPN	VPN 기동
tgw-0408d8883c27453ea	Seoul-TGW	ap-northeast-2	-	-	-
tgw-07e903d3bf6f418c4	IAD-TGW	us-east-1	-	-	-

**전송 게이트웨이 Connect 피어 상태 (2)**

ID	이름	지역	Connect 피어 중단	Connect 피어가 손상됨	Connect 피어 기동
tgw-0408d8883c27453ea	Seoul-TGW	ap-northeast-2	-	-	-
tgw-07e903d3bf6f418c4	IAD-TGW	us-east-1	-	-	-

이제 메뉴들을 살펴 봅니다. 먼저 지리적 메뉴를 선택하고 Geo Map 상태를 살펴봅니다.

Network Manager > 글로벌 네트워크 > MyNetwork > 지리적

개요 세부 정보 지리적 토플로지 이벤트 모니터링 경로 분석기

**AWS**

TGW 2  
VPC 5

연결  
VPN 0  
직접 연결 0  
Connect 피어 0

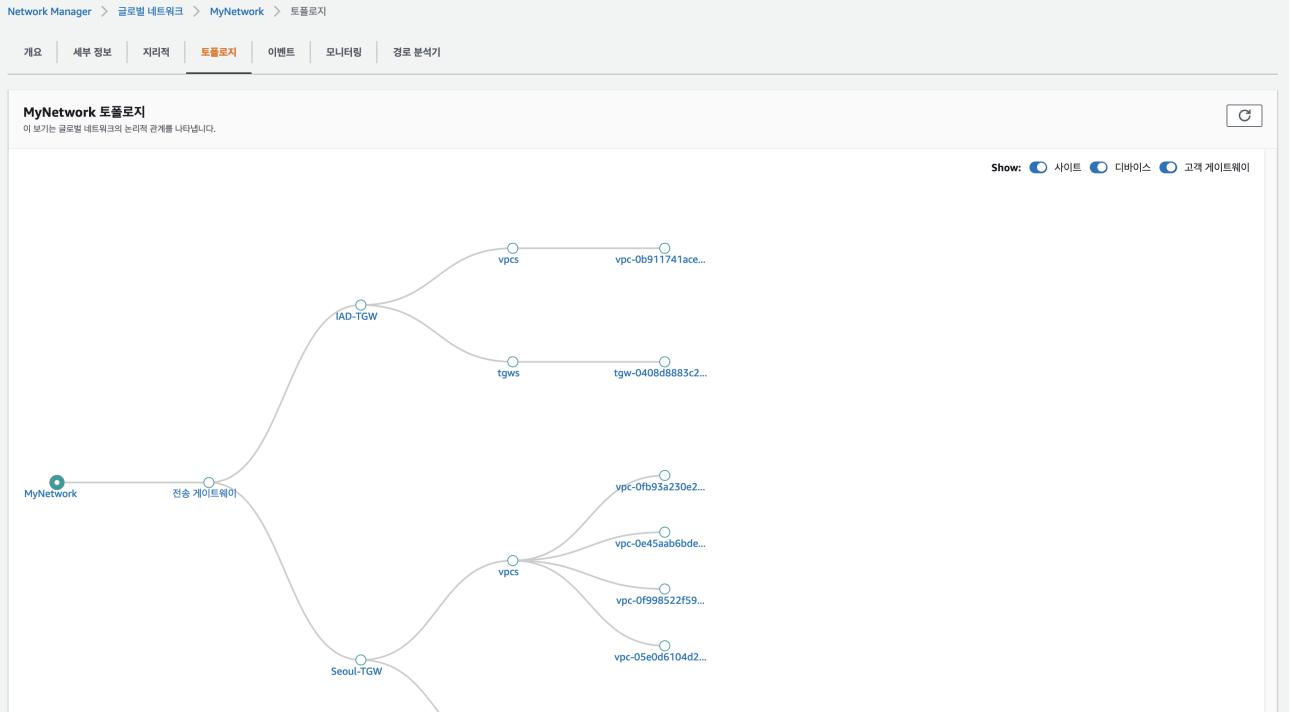
온프레미스  
사이트 0  
디바이스 0

연결되지 않음  
사이트 0  
디바이스 0

지도

지도에서 1번 위치는 미국 동부 지역, 2번 위치는 중국 동부 지역입니다.

토플로지를 선택하고, 논리적 구성도를 확인합니다.



### 3. 경로 분석기 확인

글로벌 네트워크에서 Route Analyzer를 사용하여 전송 게이트웨이 라우팅 테이블의 라우팅 분석을 수행할 수 있습니다. Route Analyzer는 지정된 소스와 대상 간의 라우팅 경로를 분석하고 구성 요소 간 연결에 대한 정보를 반환합니다. Route Analyzer를 사용하여 다음을 수행할 수 있습니다.

앞서 생성한 소스와 대상들을 입력해서 분석 결과를 살펴 봅니다.

#### 소스

- 전송 게이트웨이 : Seoul-TGW
- 전송 게이트웨이 연결 : Seoul-TGW-Attach-Seoul-VPC-PRD
- IP 주소 : 10.1.21.101

#### 대상

- 전송 게이트웨이 : Seoul-TGW
- 전송 게이트웨이 연결 : Seoul-TGW-Attach-Seoul-VPC-DEV
- IP 주소 : 10.3.21.101

Network Manager > 글로벌 네트워크 > MyNetwork > 경로 분석기

개요 | 세부 정보 | 지리적 | 토플로지 | 이벤트 | 모니터링 | 경로 분석기

**MyNetwork 경로 분석기**

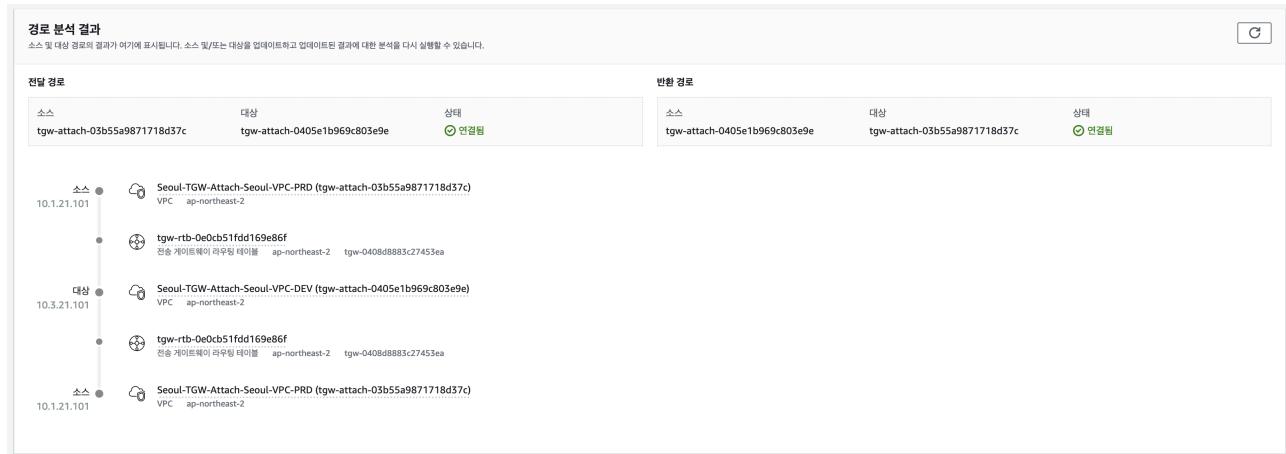
경로 분석기는 지정된 소스와 대상 간의 라우팅 경로를 분석합니다. 경로 분석기는 경로 게이트웨이 라우팅 테이블에서 경로를 확인합니다. 자세히 알아보기 [\[?\]](#)

<b>소스</b>	<b>대상</b>
전송 게이트웨이 Seoul-TGW	전송 게이트웨이 Seoul-TGW
전송 게이트웨이 연결 Seoul-TGW-Attach-Seoul-VPC-PRD	전송 게이트웨이 연결 Seoul-TGW-Attach-Seoul-VPC-DEV
IP 주소 IPv4 또는 IPv6 주소 10.1.21.101	IP 주소 IPv4 또는 IPv6 주소 10.3.21.101

결과에 반환 경로 포함  
 미출판된 애플리케이션입니다? [정보 \[?\]](#)  
 선택한 경우 결과에 알려진 것을 명시합니다.

**경로 분석 실행**

경로 분석기 결과를 확인해 봅니다.



해당 LAB의 질문 사항은 [whchoi98@gmail.com](mailto:whchoi98@gmail.com) / [whchoi@amazon.com](mailto:whchoi@amazon.com) 또는 **슬랙채널** (<https://whchoi-hol.slack.com/archives/C01QM79Q4BD>)에서 문의 가능합니다.

# TGW 자원 삭제

앞서 만들어진 자원들을 모두 삭제 합니다.

## 1. 버지니아 리전 자원 삭제

### Task1. us-east-1 Cloudformation Stack 삭제

- aws 관리콘솔 - 버지니아 북부 - Cloudformation - IAD-TGW 선택 - 삭제

스택 이름	상태	생성 시간	설명
IAD-TGW	CREATE_COMPLETE	2021-03-12 03:27:03 UTC+0900	Add Transit Gateway and TG Basic Config
IAD-VPC	CREATE_COMPLETE	2021-03-12 03:22:58 UTC+0900	-

- aws 관리콘솔 - 버지니아 북부 - Cloudformation - IAD-VPC 선택 - 삭제

### Task2. 버지니아 리전 자원 삭제 확인

EC2, VPC, TransitGateway 자원이 모두 삭제 되었는지 확인합니다.

## 2. 서울 리전 자원 삭제

### Task1. us-east-1 Cloudformation Stack 삭제

- aws 관리콘솔 - 서 - Cloudformation - Seoul-TGW 선택 - 삭제

AWS CloudFormation 스택 목록입니다. 'Seoul-TGW' 스택이 빨간색 박스로 표시되어 있으며, 상태는 'UPDATE\_COMPLETE'로 표시됩니다.

스택 이름	상태	생성 시간	설명
Seoul-GA-VPC	CREATE_COMPLETE	2021-03-11 09:59:34 UTC+0900	-
<b>Seoul-TGW</b>	<b>UPDATE_COMPLETE</b>	2021-03-10 00:05:54 UTC+0900	Add Transit Gateway and TG Basic Config
Seoul-VPC-DEV	CREATE_COMPLETE	2021-03-09 19:31:30 UTC+0900	-
Seoul-VPC-STG	CREATE_COMPLETE	2021-03-09 19:31:00 UTC+0900	-
Seoul-VPC-PRD	CREATE_COMPLETE	2021-03-09 19:30:24 UTC+0900	-
Seoul-VPC-HQ	CREATE_COMPLETE	2021-03-09 19:27:44 UTC+0900	-

- aws 관리콘솔 - 서울 - Cloudformation - VPC 선택 - 삭제 (나머지 모든 VPC들 삭제)

## Task2. 서울 리 자원 삭제 확인

EC2, VPC, TransitGateway 자원이 모두 삭제 되었는지 확인합니다.

## 3. Cloud9 자원 삭제

aws 관리콘솔 - 서울 - Cloud9에서 아래와 같이 생성된 Cloud9 IDE를 선택하고 삭제합니다.

AWS Cloud9 환경 목록입니다. 'network-account' 환경이 빨간색 박스로 표시되어 있으며, 오른쪽에 있는 'Delete' 버튼도 빨간색 박스로 표시되어 있습니다.

Your environments (1)	
<b>network-account</b>	<b>Delete</b>
Type EC2	Permissions Owner
Description No description available	
Owner Arn arn:aws:iam::[REDACTED]:user/whchoi	

TransitGateway MultiAccount 랙도 실행하였다면, 해당 계정에서 Cloudformation 스택을 삭제합니다.

# Gateway Loadbalancer

# **GWLB Overview**

# Network Firewall

# **NWFW Overview**