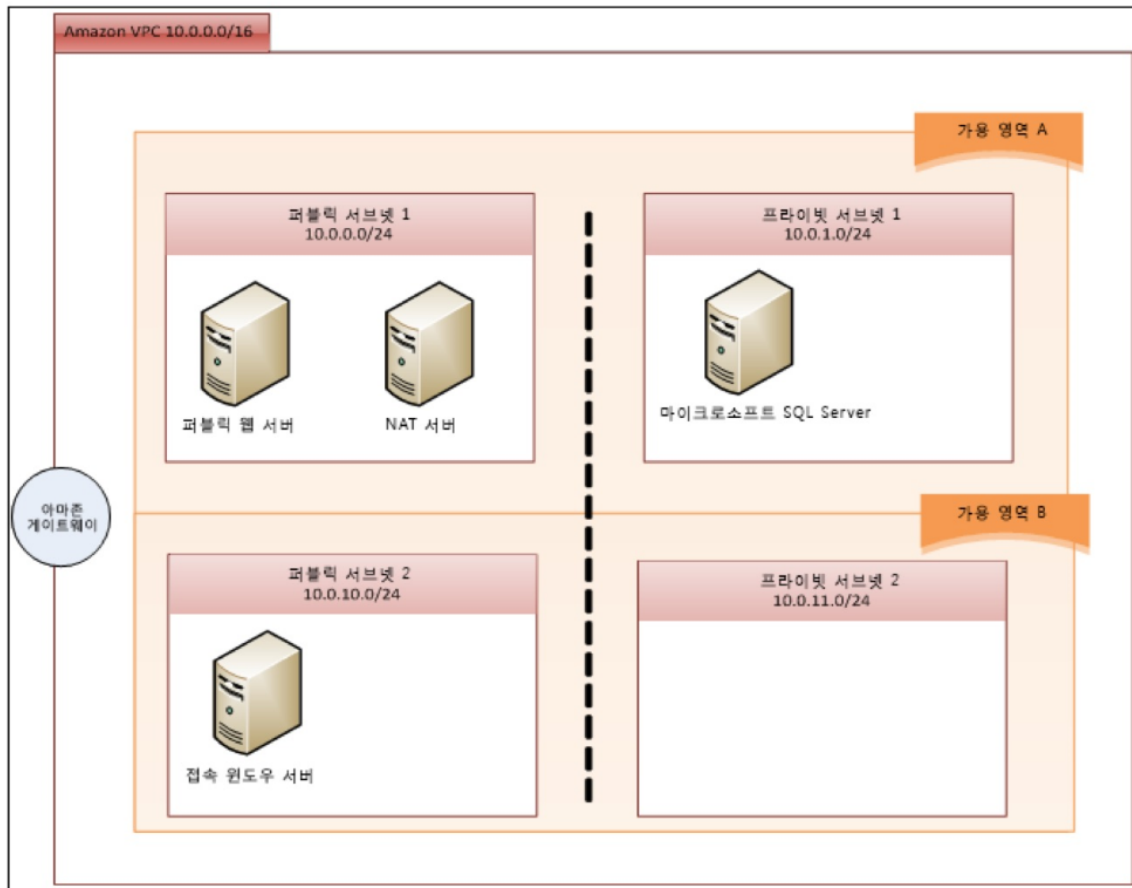


LAB 1. 처음으로 AMAZON Virtual Private Cloud 만들기

개요

본 실습 세션에서 여러분은 기본적인 Amazon Virtual Private Cloud(VPC)를 생성한 후 이를 확장하여 몇 가지 접근 및 보안관련 테스트를 수행하게 됩니다. 모든 과정은 AWS 관리 콘솔을 사용하여 수행합니다.

아래 다이어그램은 여러분이 구축할 시스템을 보여 줍니다.



전체 VPC 는 다음과 같은 다수의 기본 기능을 통합하도록 설계되었습니다.

- 이 VPC는 두 개의 가용 영역(AZ)에 걸쳐 구축되므로 향후 애플리케이션을 이러한 두 AZ로 분산시켜 애플리케이션의 내구성 및 가용성이 보장되는 아키텍처를 설계할 수 있습니다.
- 각 가용 영역(AZ) 내에는 두 개의 서브넷이 있으며, "Public" 서브넷은 인터넷에 직접 연결됩니다. "Private" 서브넷은 VPC 내 다른 서브넷과 통신할 수 있습니다. 그러나 인터넷에서 이러한 서브넷에 액세스할 수는 없습니다. 점선은 이러한 격리된 구간을 나타냅니다.

실습 시작 전 준비 사항

실습 중 일부 단계에서는 명령 줄 인터페이스를 사용해야 합니다. 이러한 단계에서는 두 가지 옵션 중 하나를 선택할 수 있습니다.

- 수동으로 명령 입력
- 이 실습에 포함된 명령 참조파일에서 해당 명령을 복사하여 붙여 넣기

이 지침에 있는 명령을 복사하여 붙여 넣는 방법은 권장하지 않습니다. 줄 바꿈 및 기타 형식으로 인해 명령이 제대로 실행되지 않을 수 있기 때문입니다. 이 문서에 기재되어 있는 모든 명령은 예시로 참조할 수만 있습니다.

qwikLAB 시작

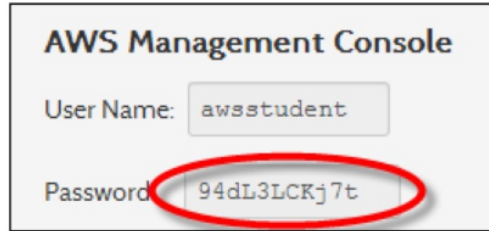
- 1) **Architecting on AWS, Day 1: Your first Virtual Private Cloud** 링크의 오른쪽에서 Start Lab 버튼을 클릭하여 qwikLAB을 시작합니다.



실습 생성 진행률을 확인할 수 있습니다.



- 2) 실습 페이지에서 실습 속성을 확인하십시오.
 - (1) **Duration** - 실습이 자동으로 종료되기 전까지 실행되는 시간입니다.
 - (2) **Setup Time** - 실습 환경을 설정하는 데 소요되는 추정 시간입니다.
 - (3) **AWS Region** - 실습 리소스가 생성되는 AWS 지역입니다.
- 3) 제공된 암호를 복사합니다.
(Tip: 표시된 값을 선택하고 CTRL+C를 누르는 것이 가장 좋은 방법입니다.)

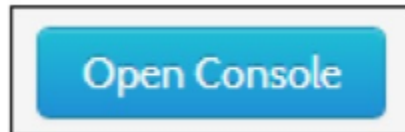


AWS Management Console

User Name:

Password:

4) **Open Console** 버튼을 클릭합니다.



5) 다음 단계에 따라 AWS 관리 콘솔에 로그인합니다.

(1) **User Name** 필드에 **awsstudent**를 입력합니다.

(2) qwikLAB의 실습 세부 정보에서 복사한 암호를 **Password** 필드에 붙여 넣습니다.

(3) **Sign in using our secure server** 버튼을 클릭합니다.



Amazon Web Services Sign In

Please enter the AWS Identity & Access Management (IAM) User name and password assigned by your system administrator to sign in.

AWS Account: 832809622232

User Name:

Password:

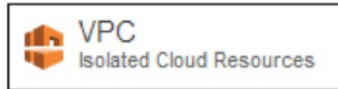
[Sign in using our secure server](#)

Please contact your system administrator if you have forgotten your user credentials.

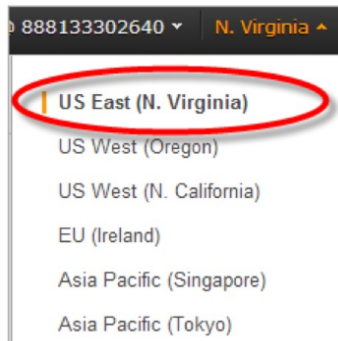
[Sign in using AWS Account credentials](#)

이 단계에서 AWS 관리 콘솔에 로그인 됩니다. **awsstudent** AWS 계정에 대한 로그인 자격 증명은 qwikLAB이 AWS Identity Access Management를 사용하여 프로비저닝 합니다.

6) 콘솔에 로그인 되면 **VPC**를 클릭합니다.

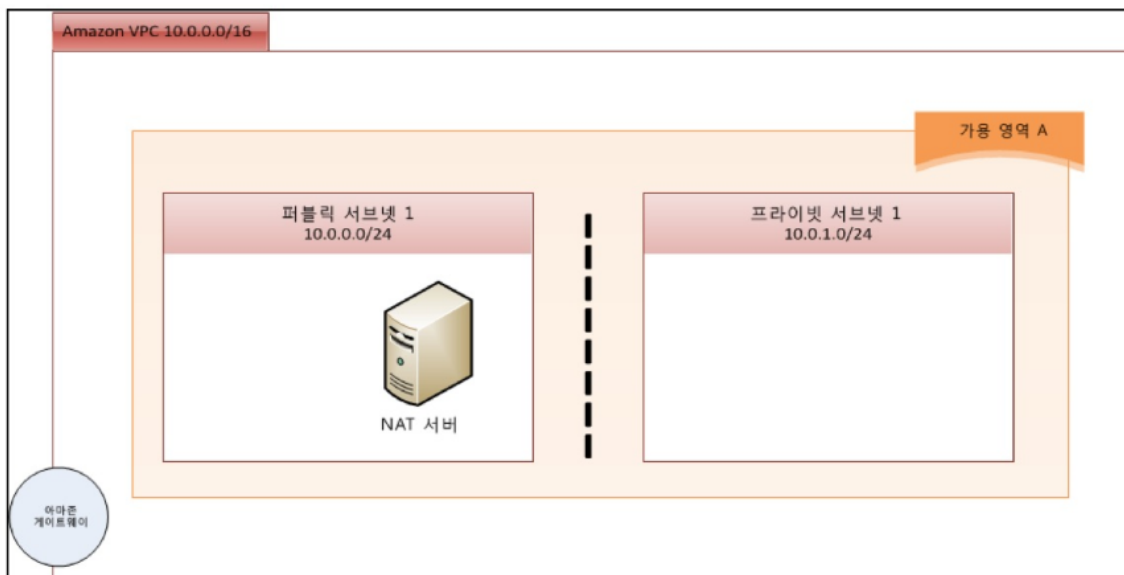


7) 실습 페이지에 표시된 것과 동일한AWS지역이AWS관리콘솔도구모음에도 표시되는지 확인합니다.



기본 VPC 생성

빠르고 사용이 간단한 마법사를 사용하여 초기 VPC 를 설정한 후 그 결과물을 수동으로 확장하는 방법을 통해 VPC 구성 옵션에 대해 자세히 알아볼 수 있습니다. 우선 다음과 같은 구성을 생성합니다.



- 1) Start VPC Wizard 버튼을 클릭합니다.
- 2) VPC with Public and Private Subnets 옵션을 선택합니다.

Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

Creates:

A /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via a Network Address Translation (NAT) instance in the public subnet. (Hourly charges for NAT instances apply.)

Select

The diagram illustrates the VPC configuration. It shows an 'Amazon Virtual Private Cloud' box containing a 'Public Subnet' and a 'Private Subnet'. The 'Public Subnet' contains a 'NAT' instance. Above the 'Public Subnet' is a cloud icon labeled 'Internet, S3, DynamoDB, SNS, SQS, etc.'. Arrows indicate connectivity from the Internet to the Public Subnet, and from the Private Subnet through the NAT instance in the Public Subnet to the Internet.

- 3) **Select** 를 클릭합니다.

"VPC with Public and Private Subnets" 창에는 여러 파라미터가 포함되어 있습니다. 여러분의 전문 배경 지식에 따라 다른 표기법이 익숙할 수도 있습니다. 이러한 표기법을 일반적으로 CIDR 블록 표기법이라고 합니다. 예를 들어 10.0.1.0/24 는 10.0.1.0 및 서브넷 마스크 255.255.255.0 으로 표현될 수도 있습니다.

VPC 자체는 10.0.0.0 공간 내 클래스 B 네트워크입니다. IPv4 어드레스 공간에 익숙하다면 이는 라우팅 될 수 없는 어드레스 블록이라는 것을 알고 계실 것입니다. 전체 어드레스 공간은 IP CIDR 블록 10.0.0.0/16 을 사용하며, 이 블록은 서브넷 마스크 255.255.0.0(전체 클래스 B 네트워크)에 해당합니다.

두 가지 예외를 제외하고는 기본값을 그대로 사용합니다.

- 4) **Edit Public Subnet**을 클릭하고 Amazon EC2 가용 영역(예: **us-east-1a**)을 선택합니다.
- 5) **Edit Private Subnet**을 클릭하고 Public 서브넷에서 선택한 것과 동일한 가용 영역을 선택 합니다.

중요: 두 서브넷이 모두 동일한 Amazon EC2 가용 영역에 있어야 합니다!

Step 2: VPC with Public and Private Subnets

IP CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

VPC name:

Public subnet:* 10.0.0.0/24 (251 IP addresses available)

Availability Zone: us-east-1a ▼

Public subnet name: Public subnet

Private subnet:* 10.0.1.0/24 (251 IP addresses available)

Availability Zone: us-east-1a ▼

Private subnet name: Private subnet

You can add more subnets after AWS creates the VPC.

Specify the details of your NAT instance.

Instance type:* m1.small ▼

Key pair name: qwiklab-l32-5040 ▼

Note: Instance rates apply. [View Rates](#).

Enable DNS hostnames:* ☒ Yes ☐ No

Hardware tenancy:* Default ▼

6) Public 및 Private Subnet 에 대해 동일한 가용 영역을 선택한 다음 **Create VPC** 버튼을 클릭하여 VPC를 생성합니다. 그러면 VPC 생성 진행률을 나타내는 대화 상자가 열립니다

7) VPC가 생성되면 **Close**를 클릭합니다.

You are using the following Amazon VPC resources in the US East (N. Virginia) region:

2 VPCs	2 Internet Gateways
8 Subnets	3 Route Tables
2 Network ACLs	1 Elastic IP
6 Security Groups	5 Running Instances
0 VPC Peering Connections	0 Customer Gateways
0 VPN Connections	0 Virtual Private Gateways

(VPC 와 Internet Gateway 숫자 이외의 항목은 화면과 다를 수 있습니다)

VPC 대시보드 에서 VPC, 두 개의 서브넷 그리고 네트워크 ACL 및 라우팅 테이블과 같은 여러 다른 기능 등이 표시됩니다. 이 시점에서 가장 중요한 점은 네트워크 환경을 사용할 준비가 되었다는 것입니다.

이뿐만 아니라 VPC 의 경우 모든 것이 단일 가용 영역 내에 있다는 점도 중요합니다. 애플리케이션 가용성을 최적화하려면 자산을 여러 영역에 걸쳐 배포해야 합니다. 다시 말하자면 다른 서브넷 페어를 추가해야 할 수도 있습니다. 이는 이 실습의 뒷부분에서 다루게 될 것입니다.

NAT 서버에서 아웃바운드 요청 처리

VPC 마법사는 마법사가 생성한 NAT 서버를 자동으로 시작합니다. NAT 서버는 Private 서브넷 내 서버가 업데이트 및 소프트웨어 패키지를 가져올 수 있도록 인터넷과 통신하도록 허용하는 것이 유일한 목적이라는 점에서 일종의 어플라이언스라 볼 수 있습니다. 이 서버는 인터넷 클라이언트가 Private 서브넷 내 서버와 연결하도록 허용하지는 않습니다. NAT 인스턴스를 생성하는 과정 중 하나로, VPC 마법사가 이를 Elastic IP 나 NAT(Network Address Translation) 또는 어드레스에 할당하여 인터넷 통신을 가능하게 합니다.

기본적으로 인스턴스 유형은 m1.small 이고 연결된 EC2 키 페어 이름은 qwikLABTM이 사용자를 위해 생성한 이름입니다. 참고: 아래의 화면 캡처는 위의 VPC 마법사에서 캡처 한 것입니다.



VPC 보안 그룹 생성

VPC 를 생성한 다음에는 VPC 보안 그룹을 생성해야 합니다.

- 1) VPC 대시보드에서 **Security Groups**를 클릭합니다.
- 2) **Create Security Group**을 클릭합니다.
- 3) Name 상자에 **WebVPCSG**를 입력합니다.
- 4) **Description** 상자에 **Web Security Group for VPC**를 입력합니다.
- 5) **VPC** 목록에서 생성한 VPC를 선택합니다. ID 뒤에 별표가 없는 VPC여야 합니다.

6) **Yes, Create** 를 클릭합니다. 그러면 VPC Security Groups 페이지에 새 보안 그룹이

보입니다.

7) Details 창에서 Inbound 탭을 클릭합니다.

8) **Edit** 버튼을 누르고 **Add another Rule** 을 눌러 목록에서 SSH를 선택한 다음 source 를 **0.0.0.0/0 (any)**으로 입력해 줍니다.

9) **Add another Rule** 을 눌러 목록에서 HTTP 를 선택한 다음 source 를 **0.0.0.0/0**으로 입력해 줍니다.

10) **Save** 를 클릭합니다.

웹 서버 시작

그 다음으로는 스탠다드 아마존 리눅스 AMI를 시작하고 웹 서버 역할을 하도록 자동 구성해야 합니다.

1) AWS 관리 콘솔의 **Services** 메뉴에서 EC2를 선택합니다.

2) **Launch Instance**를 클릭합니다.

3) 아마존 리눅스 AMI를 찾은 다음 **Select**를 클릭합니다.

4) **Instances** 창에서 **t2.micro** 인스턴스를 선택했는지 확인한 다음 **Next:Configure Instance Details** 를 클릭합니다.

5) **Configure Instance Details** 창에서 다음과 같이 진행합니다.

(1) **Network** 의 경우 생성한 VPC(**10.0.0.0/16**)를 선택합니다.

(2) **Subnet** 의 경우 Public Subnet (**10.0.0.0/24**)을 선택합니다.

(3) **Auto-assign Public IP** 항목 선택에서 **Enable** 을 선택하여 **Public IP 어드레스를**

자동으로 부여 받도록 합니다.

(4) **Advanced Details** 섹션을 확장합니다.

(이 섹션을 찾기 위해 아래로 스크롤 해야 할 수 있습니다.)

(5) User Data 필드에 다음과 같은 텍스트를 입력합니다. 여러분의 편의를 위해 이 실습에 대한 qwikLAB 페이지에 명령 참조 텍스트 파일이 첨부되어 있습니다.


```
#!/bin/sh
yum -y install httpd
chkconfig httpd on
/etc/init.d/httpd start
```

6) **Next: Add Storage** 를 클릭합니다.

7) Add Storage 창에서 변경해야 할 사항은 없습니다. 기본값을 사용하고 **Next: TagInstance** 를 클릭합니다.

8) **Tag Instance** 창의 **Key** 열에서 **Name** 행을 찾습니다. 해당 **Value** 열에 **Web Server 1**을 입력 합니다.

9) **Next: Configure Security Group**을 클릭합니다.

10) **Select an existing security group** 옵션을 선택합니다.

11) 앞에서 생성한 **WebVPCSG** 보안 그룹을 선택합니다.

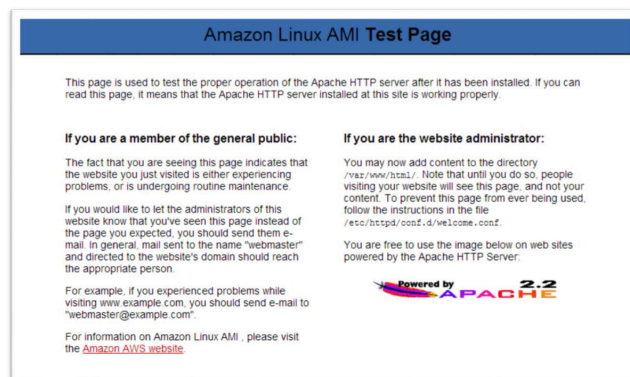
12) **Review and Launch**를 클릭합니다.

11) **Launch**를 클릭합니다. **Select an existing key pair or create a new key pair** 대화상자가 나타납니다.

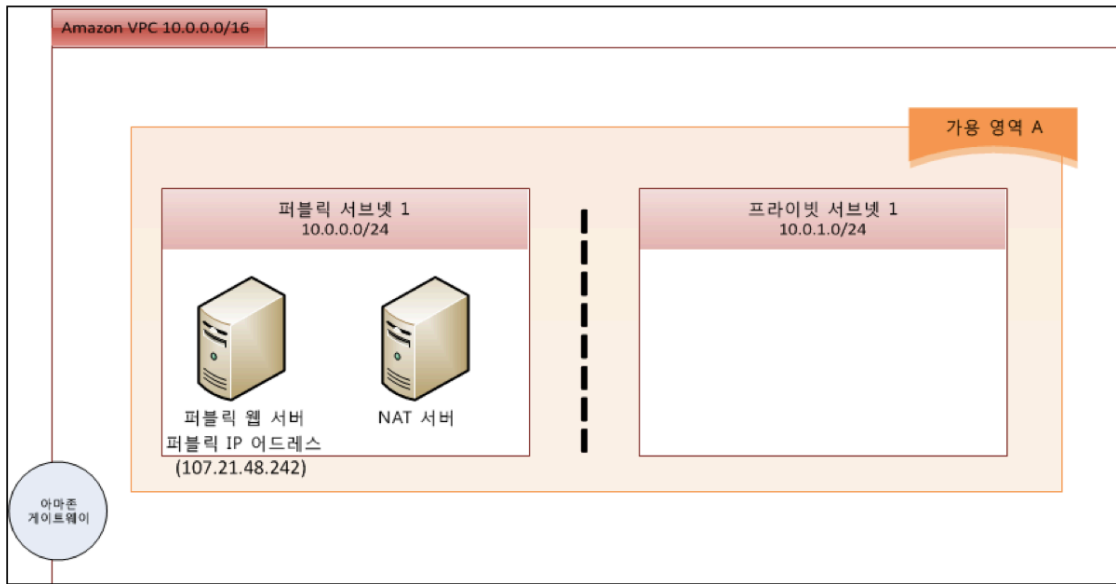
12) **Choose an existing key pair** 필드가 사용자를 위해 생성된 **qwikLAB** 키페어로 설정되어 있는지 확인한 다음 **Acknowledgement** 상자에 선택 표시를 하고 **Launch Instances**를 클릭합니다.

13) 화면의 오른쪽 하단에 있는 **View Instances**를 클릭합니다. 두 인스턴스를 확인할 수 있어야 합니다. 하나는 **Web Server 1**이라는 레이블이 지정되어 있으며, 웹 서버입니다. 다른 하나는 VPC와 함께 시작된 NAT 인스턴스입니다. 해당 인스턴스는 초기에는 'pending' 상태였다가 'running' 상태로 변경됩니다.

인스턴스가 실행되고 나면 상태 확인이 수행됩니다. 인스턴스에 **2/2 checks passed** 가 표시되면 해당 인스턴스의 **Public DNS** 어드레스를 찾아 브라우저에 이를 입력 합니다. 다음과 유사한 결과가 출력되어야 합니다.



아래 다이어그램에는 본 실습에서 지금까지 구성한 내용이 나와 있습니다.



백 엔드 마이크로소프트 SQL Server 시작

데이터베이스 보안은 매우 중요한 주제입니다. 여러분은 데이터베이스를 인터넷 트래픽과 격리된 Private 서브넷에 배치할 것입니다. 본 실습에서는 데이터베이스를 사용하지 않습니다. 대신, 서버가 제한된 조건 집합에서 RDP 를 통해 액세스할 수 있는 "지점"을 생성하는 것이 목표입니다.

- 1) EC2 대시보드를 클릭하고, **Launch Instance**를 클릭합니다.
- 2) **Microsoft Windows Server 2008 R2 with SQL Server Web AMI** 를 찾아 Select 를 선택 합니다.
- 3) Instances 창에서 **General Purpose > m3.medium**을 클릭합니다.

	Family	Type	vCPUs ①	Memory (GiB)	Instance Storage (GiB) ①
<input type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only
<input checked="" type="checkbox"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)
<input type="checkbox"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)
<input type="checkbox"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)

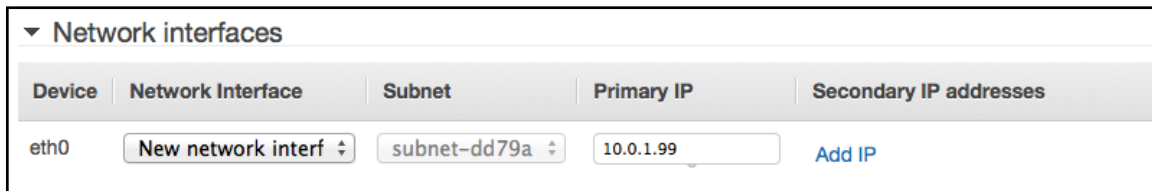
- 4) **Next: Configure Instance Details**를 클릭합니다.
- 5) **Configure Instance Details** 창에서 다음과 같이 진행합니다.

(1) Network의 경우 VPC인 10.0.0.0/16을 선택합니다.

(2) Subnet의 경우 **Private Subnet 10.0.1.0/24**를 선택합니다.

(3) 스크롤을 아래로 내려 Network Interfaces 섹션을 찾습니다. 이 섹션을 확장한 다음 디바이스를 위한 **Primary IP 필드**에 **10.0.1.99** 라는 IP 어드레스를 입력합니다.

eth0



6) **Next: Add Storage**를 클릭합니다.

7) **Add Storage** 창에서 기본값을 사용한 다음 **Next: Tag Instance**를 클릭합니다.

8) **Tag Instance** 창의 **Value 열**에 있는 **Name**에 **SQL Server**를 입력합니다.

9) **Next: Configure Security Group**을 클릭합니다.

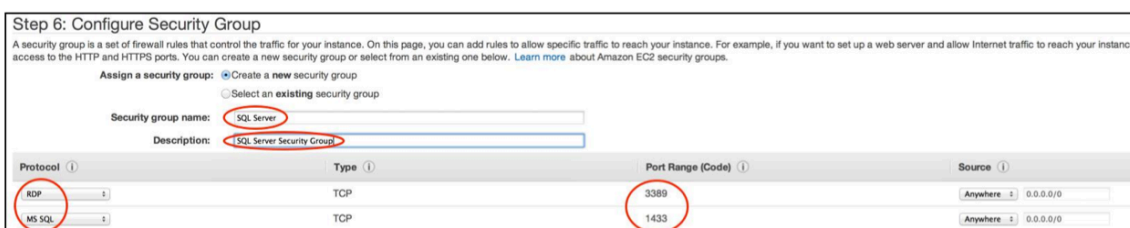
10) **Configure Security Group** 창에서 다음을 수행합니다.

(1) **Create a new security group**을 클릭합니다.

(2) **Security group name**에 **SQL Server**를 입력하고 **Description**을 추가합니다.

(3) 포트 **3389** 및 **1433**에 대한 기존 규칙이 있는지 확인합니다.

참고: 소스 IP 어드레스 범위는 "모든 곳에서 허용"을 뜻하는 0.0.0.0/0 으로 설정되어 있습니다. 라우팅 제한은 이를 "VPC 서브넷 중 하나에 존재하는 모든 호스트로부터 액세스를 허용"으로 해석합니다. 접속 인스턴스가 생성되면 이 규칙을 강화합니다.



11) **Review and Launch**를 클릭합니다.

12) Launch를 클릭한 다음 Select an existing key pair or create a new key pair 대화 상자에서 다음을 수행합니다.

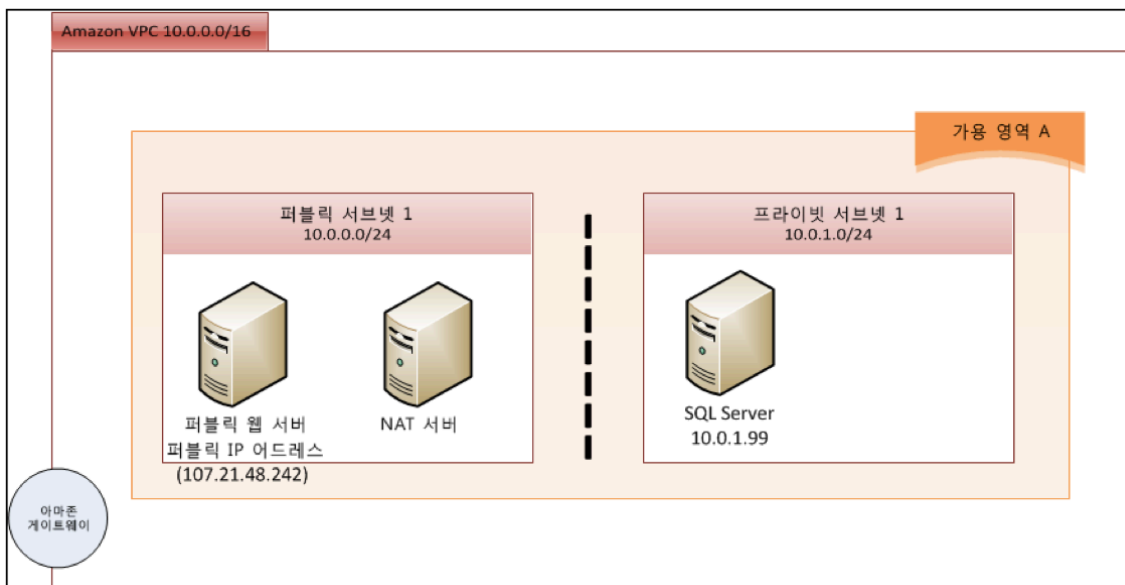
(1) Select a key pair 필드가 사용자를 위해 생성된 qwikLAB 키 페어로 설정되어 있는지 확인합니다.

(2) Acknowledgement 상자에 선택 표시를 합니다.

(3) Launch Instances를 클릭합니다.

13) View Instances를 클릭합니다. 해당 인스턴스는 초기에는 'pending' 상태였다가 'running' 상태로 변경됩니다.

여러분이 구성한 네트워크는 아래 다이어그램처럼 보일 것입니다. 데이터베이스 서버가 웹 서버 역할을 하도록 설정되어 있지 않기 때문에 이 네트워크는 아직 서비스 가능한 상태는 아니며 SQL Server 를 연결하고 관리할 안전한 방법이 필요합니다. NAT 는 SQL Server 가 윈도우 업데이트 등을 다운로드하기 위한 아웃바운드 인터넷 호출을 허용하는 라우터로 작동하게 됩니다.



이 환경에는 또 하나의 매우 중요한 요소, 즉 다른 웹 서버와 보조 데이터베이스 서버가 포함된 보조 가용 영역이 빠져 있습니다. AWS 는 추가 비용 없이 다중 가용 영역에 대한 액세스를 제공합니다. 모범 사례는 두 개의 영역에서 서버를 미러링 한 후 로드 밸런싱 등의 기법을 사용하여 두 영역 간에 트래픽을 분산하는 것입니다.

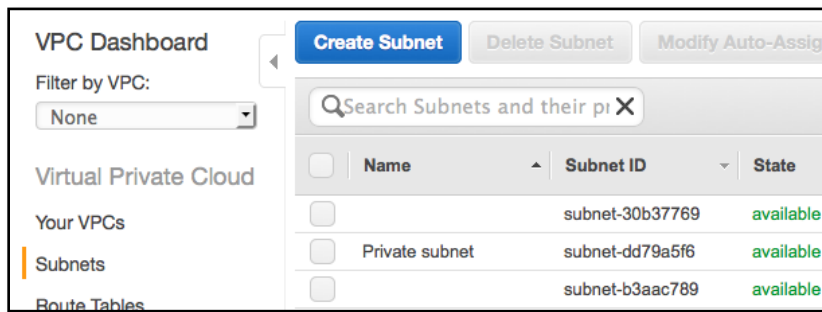
AWS 는 다중 AZ 배포가 사용자에게 반드시 필요하다고 생각하고 있습니다. 당사의 데이터 센터는 일반적인 엔터프라이즈 데이터 센터에 비해 보다 안정적이지만 장애는 발생할 수

있는 것입니다. 환경이 단일 AZ 라면 SLA 보호가 없습니다. EC2 SLA 는 동일한 AWS 지역에서 두 개 이상의 가용 영역에 인스턴스를 실행하고 있고, 이러한 가용 영역이 동시에 오프라인 되는 경우에만 유효합니다.

수동으로 두 개 이상의 서브넷 생성

이제 또 다른 가용 영역에서 Public 서브넷과 Private 서브넷을 생성해야 합니다. 이전의 서브넷과 달리, 이들 서브넷은 마법사 도움 없이 생성합니다. 이 과정에서 서브넷이 작동하는 방식을 더 자세히 학습할 수 있을 것입니다. 이들 서브넷은 모두 동일한 가용 영역에 배치되지만, 앞서 생성한 두 서브넷과는 다른 가용 영역입니다. 참고로, 원래의 서브넷은 10.0.0.0/24(Public)와 10.0.1.0/24(프라이빗)였습니다. 두 서브넷은 동일한 가용 영역에 있었습니다.

- 1) AWS 관리 콘솔의 **Services** 메뉴에서 **VPC**를 선택합니다.
- 2) **Virtual Private Cloud** 섹션에서 **Subnets**를 클릭하고 **Create Subnet**을 클릭합니다.



- 3) 이전 단계에서 알게 된 사항을 바탕으로 다음을 수행합니다.
 - (1) 생성한 VPC 내에 CIDR 블록 10.0.10.0/24를 사용하여 새로운 Public 서브넷을 생성합니다.
 - (2) Availability Zone의 경우 이전 Public 서브넷에서 사용했던 영역과 다른 영역을 선택하십시오.

참고: AZ가 제각각 다를 수 있으며, 이전에 선택하지 않았던 곳으로 선택합니다.

The screenshot shows the 'Create Subnet' dialog box. It includes a header with a question mark and a close button. Below the header is a note about CIDR format. The form contains four fields: 'Name tag' (empty), 'VPC' (vpc-6924520c (10.0.0.0/16) | LAB Test), 'Availability Zone' (us-east-1c), and 'CIDR block' (10.0.10.0/24). At the bottom right, there are 'Cancel' and 'Yes, Create' buttons.

4) Yes, Create를 클릭합니다.

5) 위 단계를 반복하여 CIDR 블록 10.0.11.0/24를 사용하는 새 Private 서브넷을 생성합니다.
(이 서브넷은 반드시 Public 서브넷과 동일한 가용 영역에 배치해야 합니다.)

서브넷을 Public 또는 Private 으로 결정짓는 요소는 무엇일까요?

이제 두 개의 서브넷을 추가로 생성했습니다. 하지만 무엇을 사용해 이 두 개의 서브넷을 Private 또는 Public으로 구분합니까? 바로 라우팅 규칙입니다.

1) CIDR 10.0.0.0/24를 사용하는 서브넷을 선택하고 Route Table(아래 Details 탭에 있음)에 두 개의 라우팅 규칙이 있는 것을 확인하십시오.

- 이 서브넷 안의 모든 머신은 10.0.0.0/16내 다른 모든 머신과, 전체 VPC와 통신할 수 있습니다. 다시 말해 모든 서브넷 간 통신에 제한이 없습니다. 이 실습의 뒷부분에서 트래픽을 제한하기 위한 메커니즘으로서 보안 그룹을 살펴볼 것입니다.
- 인터넷(0.0.0.0/0)을 통해 주고받는 모든 트래픽은 인터넷 게이트웨이 디바이스를 통해 라우팅 됩니다. 이제까지 이 디바이스를 본 적은 없지만 이를 VPC의 엣지에 있는 라우터로 생각하면 됩니다. 네트워크 다이어그램에도 그렇게 그려져 있습니다.

2) 또한, Network ACLs 항목을 살펴보면 네트워크 ACL이 보입니다. 이론상 이들 ACL도 트래픽을 제어할 수 있습니다. 하지만 VPC에서는 제한된 수의 규칙만 지원하므로 우리는 더욱 세분화된 대체 제어를 사용합니다.

Search Subnets and their p X

<input type="checkbox"/>	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone
<input checked="" type="checkbox"/>	subnet-d679a5fd	available	vpc-6924520c (10.0.0.0/16) LAB Test	10.0.0.0/24	249	us-east-1a
<input type="checkbox"/>	subnet-dd79a5f6	available	vpc-6924520c (10.0.0.0/16) LAB Test	10.0.1.0/24	250	us-east-1a
<input type="checkbox"/>	subnet-f10bbda8	available	vpc-6924520c (10.0.0.0/16) LAB Test	10.0.10.0/24	251	us-east-1c
<input type="checkbox"/>	subnet-ef0bbdb6	available	vpc-6924520c (10.0.0.0/16) LAB Test	10.0.11.0/24	251	us-east-1c

subnet-d679a5fd (10.0.0.0/24) | Public_1a

Summary Route Table Network ACL Tags

Edit

Route Table: [rtb-37430352](#)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-40c37825

3) 10.0.1.0/24 서브넷을 선택합니다. 마찬가지로 10.0.1.0/24에도 다음과 같은 라우팅 규칙이 있습니다.

- VPC(10.0.0.0/16) 내 다른 모든 서브넷으로 가는 트래픽은 제한되지 않습니다.
- 인터넷으로 향하는 트래픽은 NAT 인스턴스인 EC2 인스턴스로 이어집니다.

NAT는 인터넷으로부터의 무작위 요청을 이 서브넷으로 다시 라우팅하지 않는다는 점에 유의하십시오. 이 서브넷 내부로부터의 아웃바운드 요청에 대한 응답만 라우팅 합니다.

Search Subnets and their p X

<input type="checkbox"/>	Subnet ID	State	VPC	CIDR	Available IPs
<input type="checkbox"/>	subnet-d679a5fd	available	vpc-6924520c (10.0.0.0/16) LAB Test	10.0.0.0/24	249
<input checked="" type="checkbox"/>	subnet-dd79a5f6	available	vpc-6924520c (10.0.0.0/16) LAB Test	10.0.1.0/24	250
<input type="checkbox"/>	subnet-f10bbda8	available	vpc-6924520c (10.0.0.0/16) LAB Test	10.0.10.0/24	251
<input type="checkbox"/>	subnet-ef0bbdb6	available	vpc-6924520c (10.0.0.0/16) LAB Test	10.0.11.0/24	251

subnet-dd79a5f6 (10.0.1.0/24) | Private_1a

Summary Route Table Network ACL Tags

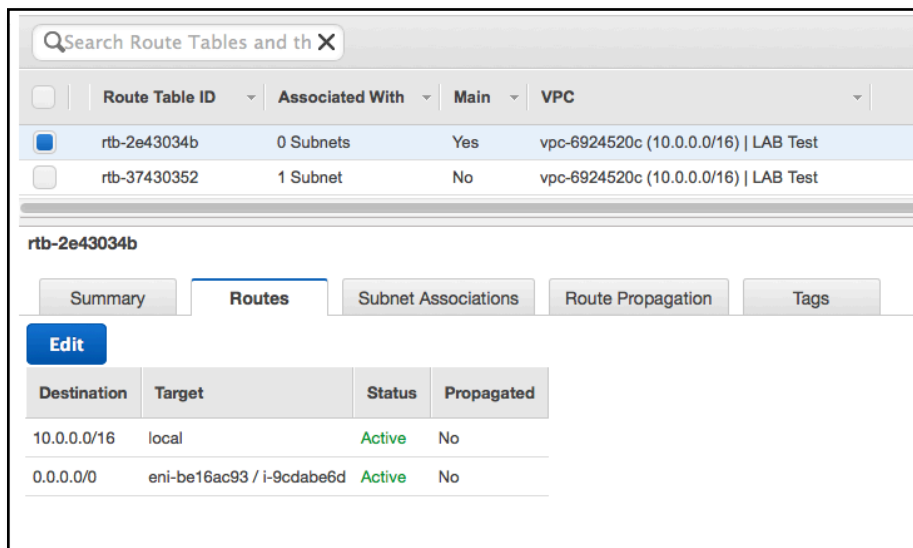
Edit

Route Table: [rtb-2e43034b](#)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	eni-be16ac93 / i-9cdabe6d

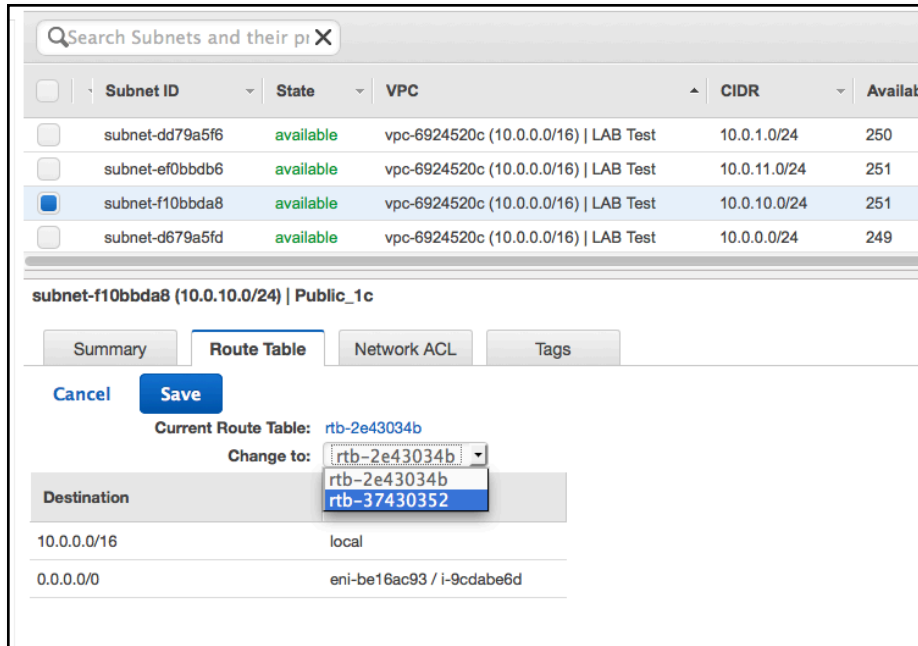
4) **Virtual Private Clouds** 섹션에서 **Route Tables**를 클릭합니다. 이 보기에 따르면 모든 라우팅 규칙에 1개의 서브넷만 연결되어 있지만, 서브넷은 모두 4개입니다. 그 이유는 무엇일까요?

Amazon VPC 는 "안전제일" 원칙에 따라 운영됩니다. 규칙 세트 중 하나가 "main"으로 표시되었음에 유의하십시오. 서브넷이 라우팅 규칙 세트와 명시적으로 연결되지 않은 경우 해당 서브넷은 기본 규칙 세트를 사용하며 이 규칙 세트는 인터넷과 통신하지 않습니다. 따라서 기본적으로 어떤 서브넷도 인터넷과 통신할 수 없습니다(기본 동작을 변경하지 않는 한).

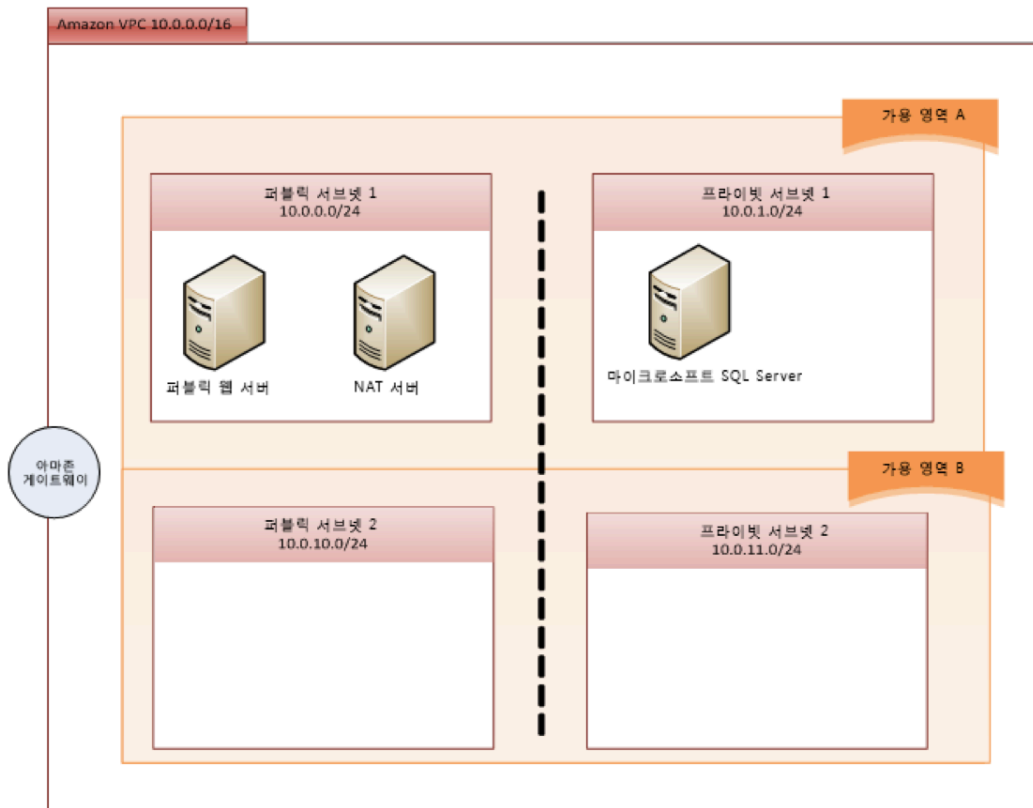


5) 이제 새 Public 서브넷(10.0.10.0/24)을 인터넷과 양방향으로 라우팅 하는 라우팅 규칙 세트와 연결해야 합니다. Subnets를 클릭하고 10.0.10.0/24 서브넷을 선택합니다.

6) Route Table의 윗 쪽에 있는 Edit을 클릭하고 **Route Table**을 **Change to** 로 다른 **Table**로 교체한 후 **Save** 를 클릭합니다.



이제 VPC 는 다음과 같이 보일 것입니다.



접속 윈도우 호스트 시작

접속 호스트는 무단 네트워크 액세스를 방지하도록 구성된 컴퓨터이며, 방화벽 앞 또는 기업 DMZ 내에 위치하는 경우가 많습니다. 접속 호스트는 일반적으로 매우 제한적인 수의 서비스(예: 프록시 서버)를 실행하므로 침입 당할 수 있는 네트워크 진입 점이 보다 적습니다. 여러분은 접속 호스트를 새로운 Public 서브넷에 생성하게 되겠지만 원래의 Public 서브넷도 무방합니다.

- 1) VPC 대시보드 를 클릭한 다음 **Launch EC2 Instances** 버튼을 클릭합니다.
- 2) **Launch Instance**를 클릭하여 새 인스턴스 마법사를 엽니다.
- 3) **Windows Server 2008 R2 Base AMI**를 선택합니다.
- 4) **Instances** 창에서 **General Purpose**를 클릭하고 **t2.medium**을 선택한 다음 **Next: Configure Instance Details**를 클릭합니다.
- 5) **Network** 목록에서 **10.0.0.0/16**을 선택합니다.
- 6) **Subnet** 목록에서 **10.0.10.0/24**를 선택합니다.
- 7) **Auto-assign Public IP** 항목에서 **Enable** 을 선택하여 이 인스턴스에 Public IP 어드레스를 자동으로 부여합니다.
- 8) **Next: Add Storage**를 클릭합니다.
- 9) **Next: Tag Instance**를 클릭합니다.
- 10) 인스턴스에 **Bastion Host**라는 Name 태그를 부여합니다.
- 11) **Next: Configure Security Group**을 클릭합니다.
- 12) **Configure Security Group** 창에서 **Bastion SG**라는 이름의 새로운 보안 그룹을 생성합니다. 그러면 윈도우 원격 데스크톱 프로토콜(RDP)인 포트 3389에 대한 액세스만 허용됩니다. 이 실습에서는 인터넷의 모든 IP 어드레스로부터의 액세스를 허용합니다. 실제 상황에서 사용할 때는 관리가 필요한 어드레스 범위로 액세스를 제한할 수 있습니다.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Protocol	Type	Port Range (Code)	Source
RDP	TCP	3389	Anywhere 0.0.0.0/0

13) **Review and Launch**를 클릭합니다.

14) **Launch**를 클릭합니다.

15) **qwikLAB** 키 페어를 선택한 다음 **Acknowledgement**에 선택 표시를 하고 **Launch Instances**를 클릭합니다.

16) **View Instances**를 클릭합니다.

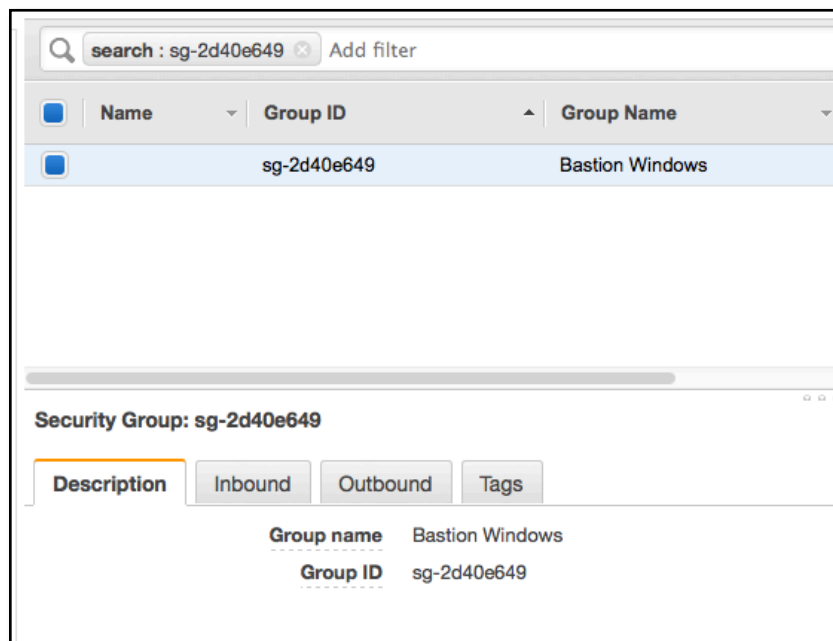
이제 접속 서버의 보안 그룹을 설정했으므로 데이터베이스 서버 규칙을 변경하여 접속 보안 그룹으로부터의 트래픽 만 수락하도록 합니다.

데이터베이스 서버 구성

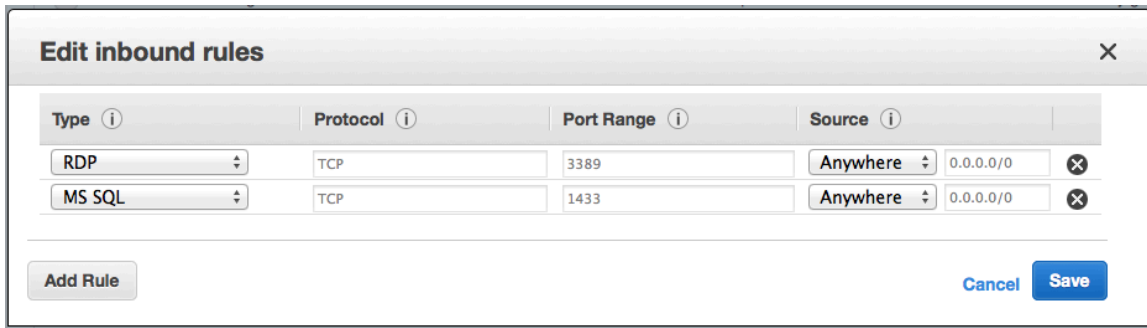
1) EC2 대시보드 에서 **Security Groups**를 클릭합니다.

2) **Bastion Windows** 보안 그룹을 선택하고 아래의 **Details** 탭을 봅니다.

3) **Bastion Windows** 보안 그룹의 **Group ID**를 기록합니다(이후 사용해야 함). 메모장 문서에 붙여 넣거나 클립보드에 복사할 수 있습니다.

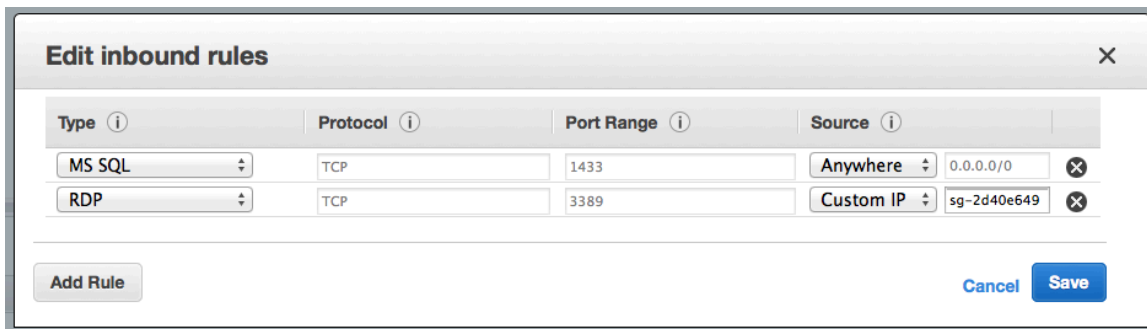


4) SQL Server 보안 그룹을 선택하고 아래의 Inbound 탭으로 전환한 후, 0.0.0.0/0으로 되어있는 Source 를 앞에서 기록해 둔 Bastion Windows 의 보안그룹으로 대체합니다.



Type	Protocol	Port Range	Source
RDP	TCP	3389	Anywhere 0.0.0.0/0
MS SQL	TCP	1433	Anywhere 0.0.0.0/0

Add Rule Cancel Save



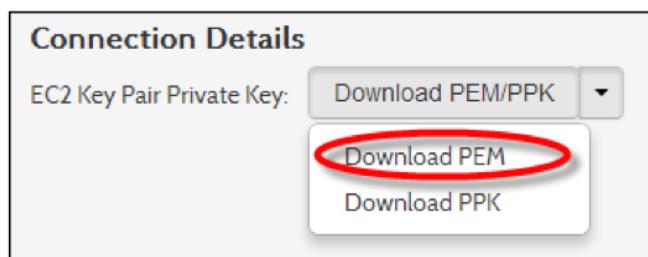
Type	Protocol	Port Range	Source
MS SQL	TCP	1433	Anywhere 0.0.0.0/0
RDP	TCP	3389	Custom IP sg-2d40e649

Add Rule Cancel Save

6) Save 를 클릭하여 변경 내용을 적용합니다.

윈도우 암호 찾기

- 1) 브라우저에서 qwikLAB 탭으로 전환합니다.
- 2) EC2 Key Pair Private Key에 대해 드롭 다운 목록에서 Download PEM을선택합니다. 그러면 qwikLAB에서 제공하는 EC2 키 페어 Private 키를 PEM 형식으로 다운로드 합니다.



3) 이 파일을 컴퓨터의 WDownloads 폴더(기본값)에 저장하거나 원하는 폴더 또는 디렉터리로 옮깁니다.

4) EC2 Management Console 탭으로 전환합니다.

5) Instances 섹션에서 Instances 링크를 클릭합니다.

6) Bastion Windows Host 인스턴스 를 마우스 오른쪽 버튼으로 클릭하고 Get Windows Password를 선택합니다.

참고: 윈도우 암호가 생성될 때까지 수 분이 걸릴 수 있습니다. 암호가 아직 준비되지 않은 경우 "not available yet"이라는 메시지가 표시됩니다. Close 를 클릭하고 잠시 기다렸다가 **Get Windows Password** 를 다시 선택합니다.

7) **Choose File**을 선택하고 %Downloads 폴더(또는 사용자의 다운로드 디렉터리/폴더)를 탐색하여 qwikLAB으로부터 다운로드 한 EC2 키 페어 Private 키(.pem) 파일을 선택합니다.

8) **Decrypt Password**를 클릭합니다.

9) IP 어드레스, 사용자 이름, 암호를 적어 놓습니다. 이 항목들은 나중에 필요하므로 텍스트 파일에 붙여 넣는 것이 좋습니다.

접속 서버 연결(윈도우)

중요: 리눅스 기반 노트북을 사용하여 이 실습을 수행할 경우 이후에 나오는 "접속 서버 연결(OS X)" 또는 "접속 서버 연결(리눅스)" 섹션 중 하나로 이동합니다. 본 섹션은 마이크로소프트 윈도우 사용자만을 위한 설명입니다. 각 섹션의 단계를 수행할 필요는 없습니다. 현재 운영 체제와 일치하는 섹션만 수행하십시오.

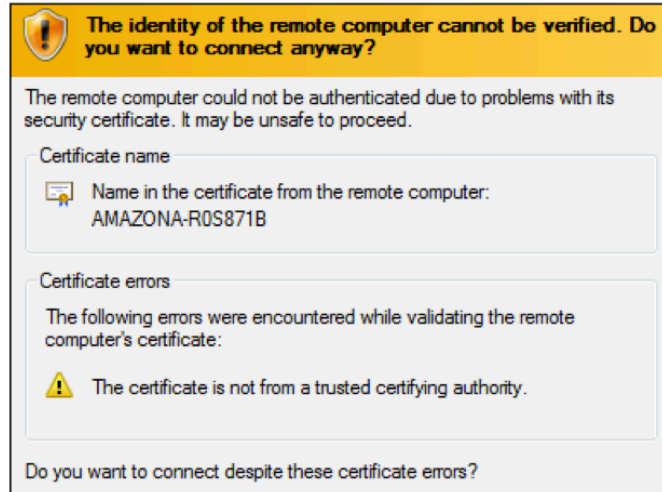
1) 로컬 컴퓨터에서 Start > Run을 클릭하고 MSTSC를 입력한 후 OK를 클릭하여 로컬 RDP 클라이언트를 시작합니다.

2) Show Options를 클릭한 다음 기록해 둔 IP 어드레스를 입력하거나 붙여 넣고 Connect를 클릭합니다.

참고: 여러분은 다른 사용자 즉 Administrator 로 로그인 중이며, 로컬 컴퓨터의 관리자 사용자와 구별하기 위해 사용자 이름을 "%Administrator"(앞에 백슬래시가 붙음)로 지정해야 할 수도 있습니다.

3) 프롬프트가 표시되면 메모해 둔 **암호**를 입력합니다.

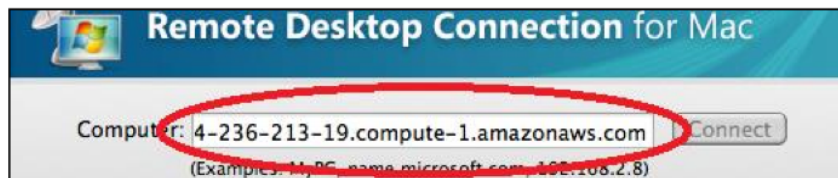
4) "원격 컴퓨터의 ID를 확인할 수 없습니다."와 유사한 인증 확인 메시지가 나타나면 **예**를 클릭합니다.



접속 서버 연결(OS X)

중요: 이전 섹션을 완료했다면 이 단계를 완료하지 않아도 됩니다. "데이터베이스 서버 로그인" 섹션으로 이동하십시오. 이 섹션은 OS X 사용자만을 위한 설명입니다. 다른 리눅스 기반 운영 체제를 사용할 경우 "접속 서버 연결(리눅스)" 섹션으로 이동하십시오. 각 섹션의 단계를 수행할 필요는 없습니다. 현재 운영 체제와 일치하는 섹션만 수행하십시오.

- 1) Remote Desktop Connection for Mac 애플리케이션을 엽니다.
- 2) 접속 컴퓨터의 IP 어드레스를 입력한 다음 Connect를 클릭합니다.



- 3) 프롬프트가 표시되면 메모해 둔 사용자 이름과 암호를 입력합니다. 도메인은 EC2 Instance DNS라고 자동 입력되므로 무시하십시오.

User name:	Administrator
Password:	••••••••
Domain:	ec2-54-236-213-19.compute-1.

- 4) OK를 클릭합니다.
- 5) "The server name is incorrect."와 유사한 확인 메시지가 나타나면 Connect를 클릭합니다.

6) "데이터베이스 서버 로그인" 섹션으로 이동합니다.

데이터베이스 서버 로그인

현재 Public 서브넷에 있는 접속 호스트 컴퓨터에 연결된 상태입니다. 다음 단계는 접속 호스트에서 SQL Server 로 연결하는 것입니다.

1) 윈도우 암호 찾기의 단계를 참조하여 SQL Server 인스턴스에 대한 암호를 찾습니다.

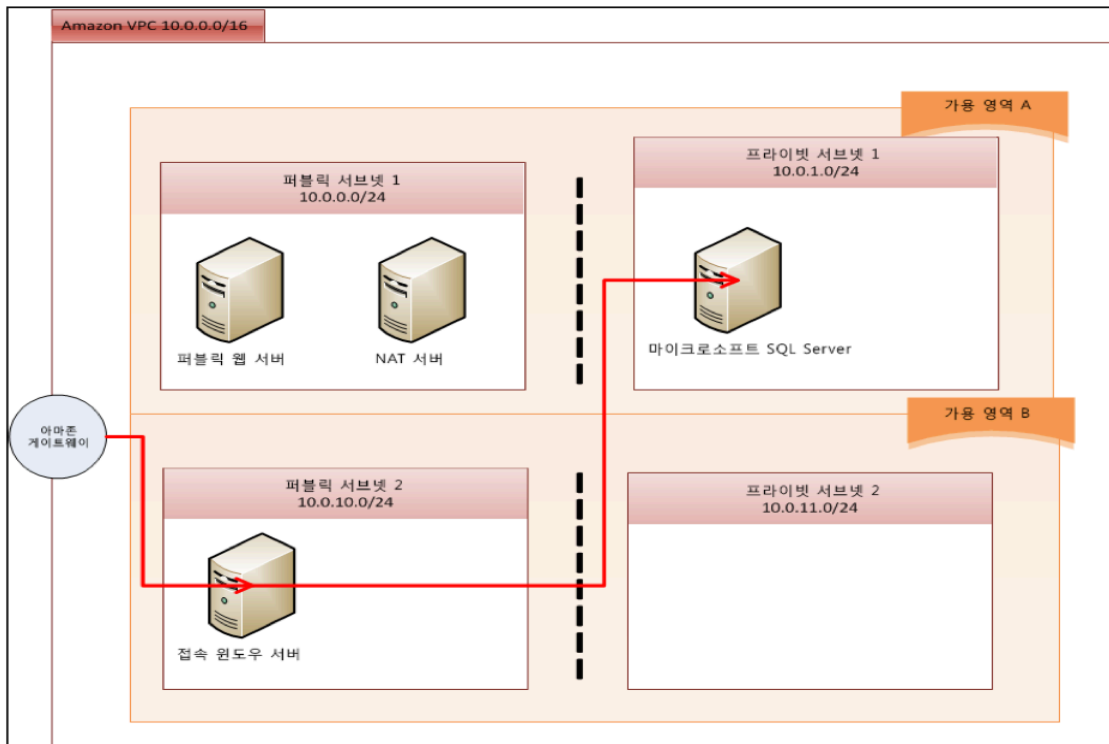
2) 접속 호스트에 연결합니다.

3) 윈도우 접속 호스트에 로그인 되어 있으므로 이전의 윈도우 연결 단계를 반복하여 접속 호스트 세션에서 SQL Server 인스턴스로 로그인합니다. 로컬에서 OS X 또는 리눅스를 실행하는 경우라도 "접속 서버 연결(윈도우)" 단계를 사용해야 합니다. 그 이유는 원격 윈도우 접속 호스트 내에서 RDP 클라이언트를 실행 중이기 때문입니다.

4) Remote Desktop Client의 **Computer 필드에 10.0.1.99를 입력합니다**. 이제 SQL Server 에 성공적으로 연결할 수 있어야 합니다. SQL Server 가 Private 서브넷에 있는 동안에는 접속 서버를 통한 연결이 가능합니다.

축하합니다!

여러분이 완성한 환경은 다음과 같을 것입니다. 게이트웨이 디바이스에서 SQL Server 까지의 경로는 VPC 네트워크의 엣지로부터 접속 호스트를 통과하여 SQL Server 까지 이어지는 트래픽 흐름을 나타냅니다. 여러분은 왜 보조 Private 서브넷(다이어그램에서 Private Subnet 2 (10.0.11/0/24) 라는 레이블이 지정된 서브넷)을 생성했는지 그 이유가 궁금할 것입니다. 이 서브넷 에서 Private Subnet 1(10.0.1.0/24)에 있는 SQL Server 의 복제를 생성할 수 있습니다.



추가 작업

이제 SQL Server 에 연결되었으므로 웹 브라우저를 열고 웹 사이트로의 연결을 시도합니다. 해당 연결이 작동하지 않음을 알 수 있습니다. 추가 도전 과제는 왜 이 연결이 거절되었는지 알아내는 것입니다. 힌트: NAT 서버 및 SQL Server 에서의 AWS 보안 그룹 설정과 관련이 있습니다.

결론

지금까지 살펴본 바에 의하면 Private 서브넷에 있는 서버에 대한 액세스를 제어하는 방법은 여러 가지가 있습니다. 네트워크가 안전할 수 있으려면 서버가 배치된 서브넷에 주의를 기울여야 합니다.

접속 호스트와 VPN 터널에는 각각 장점이 있습니다. 접속 호스트는 서버를 관리하기 위해 안전하게 로그인하는 방법을 제공하므로 특히 소수의 인원이 이 작업을 수행해야 하는 경우 이상적입니다. VPC 를 기업 네트워크에 대한 가상 확장으로 활용하고자 하는 경우에는 VPN 이 더 적합할 수 있습니다.

마지막으로 보안 그룹 규칙은 매우 엄격하거나 매우 느슨할 수 있다는 점을 배웠습니다. 보안 그룹을 가능한 한 제한적으로 설정해야 하지만 의도하지 않은 부작용이 발생할 만큼 지나치게 제한적이지는 않도록 해야 합니다.