Amazon Virtual Private Cloud

시작 안내서

API Version 2015-04-15

Amazon Virtual Private Cloud: 시작 안내서

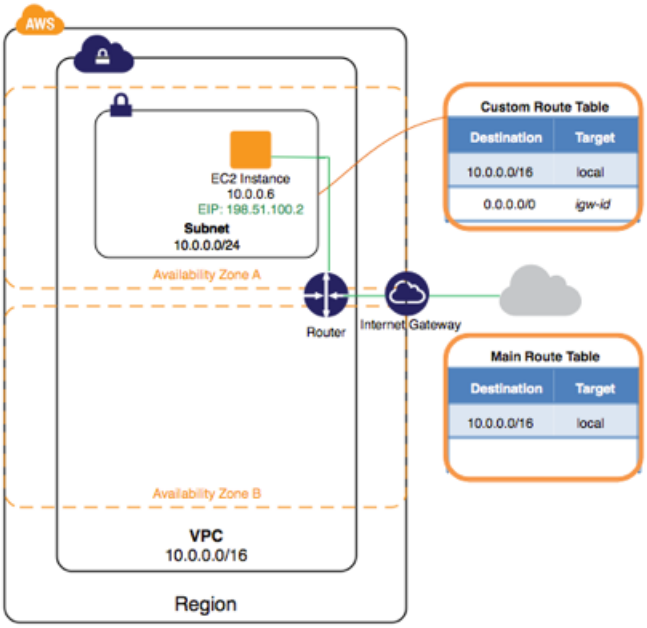
Table of Contents

개요

가상 사설 클라우드(VPC)는 자체 데이터 센터에서 운영하는 기존 네트워크와 매우 유사한 가상 네트워크로서, Amazon Web Services(AWS)의 확장 가능한 인프라를 이용할 수 있다는 이점이 있습니다. 이 연습의 해당 작업들을 완료한 후에는 VPC에서 실행되는 Amazon EC2 인스턴스를 갖게 되는데, SSH(Linux 인스턴스용) 또는 원격 데스크톱(Windows 인스턴스용)을 사용하면 인터넷을 통해 이 인스턴스에 액세스할 수 있습니다.

Amazon VPC의 개요는 What is Amazon VPC?(출처: *Amazon VPC 사용 설명서*)를 참조하십시오.

아래의 도표는 이 안내서의 연습을 완료하면 생성되는 아키텍처입니다. 인스턴스와 연결되도록 설정된 보안 그룹은 특정 포트를 통하는 트래픽만을 허용하여 지정된 규칙을 따르는 인스턴스와의 통신으로 제한합니다. 엘라스틱 IP 주소(EIP)를 사용하면 본래 사설 서브넷인 VPC의 인스턴스가 인터넷 게이트웨이를 통해서 인터넷 연결이 가능합니다. 예를 들면 웹 서버로 동작할 수 있습니다.



Amazon VPC 시작하기

이 연습에서는 VPC와 서브넷을 만든 후 해당 서브넷에서 퍼블릭 인스턴스를 시작합니다. 인스턴스는 인터넷과 통신할 수 있으며, SSH(Linux 인스턴스인 경우) 또는 원격 데스크톱(Windows 인스턴스인 경우)을 사용하여 로컬 컴퓨터에서 이러한 인스턴스에 액세스할 수 있어야 합니다. 실제 환경에서는 이 시나리오를 사용하여 블로그 호스팅과 같은 퍼블릭 웹 서버를 만들 수 있습니다.

Note

이 연습은 기본이 아닌 VPC를 직접 신속하게 설정하는 과정을 안내해 줍니다. 기본 VPC가 이미 있으며 이 VPC에서 인스턴스를 시작하려는 경우(새로운 VPC를 만들거나 구성하지 않을 경우), 기본 VPC로 EC2 인스턴스 시작 단원을 참조하십시오.

이 연습을 완료하려면 다음 작업을 수행하십시오.

- 단일 퍼블릭 서브넷이 포함된 기본이 아닌 VPC를 만듭니다. 서브넷을 사용하면 보안 및 운영상의 필요에 따라 인스턴스를 그룹화할 수 있습니다. 퍼블릭 서브넷은 인터넷 게이트웨이를 통해 인터넷에 액세스할 수 있는 서브넷입니다.
- 특정 포트를 통해서만 트래픽을 허용하는 인스턴스의 보안 그룹을 만듭니다.
- Amazon EC2 인스턴스를 서브넷에서 시작합니다.
- 인스턴스와 엘라스틱 IP 주소 연결. 이렇게 하면 인스턴스가 인터넷에 액세스할 수 있습니다.

Amazon VPC를 처음 사용할 경우, 먼저 Amazon Web Services (AWS)에 가입해야 합니다. 가입 시 AWS 계정은 Amazon VPC를 포함해 AWS의 모든 서비스에 자동으로 등록됩니다. AWS 계정을 아직 만들지 않은 경우 http://aws.amazon.com으로 이동한 후 무료 계정 생성을 선택합니다.

Note

이 연습에서는 해당 계정에서 EC2-VPC 플랫폼만 지원하는 것으로 가정합니다. 계정이 이전 EC2-Classic 플랫폼도 지원할 경우 이 연습의 단계를 그대로 진행해도 됩니다. 하지만 이 경우 해당 계정에 기본이 아닌 VPC와 비교할 기본 VPC가 없습니다. 자세한 내용은 지원되는 플랫폼을 참조하십시오.

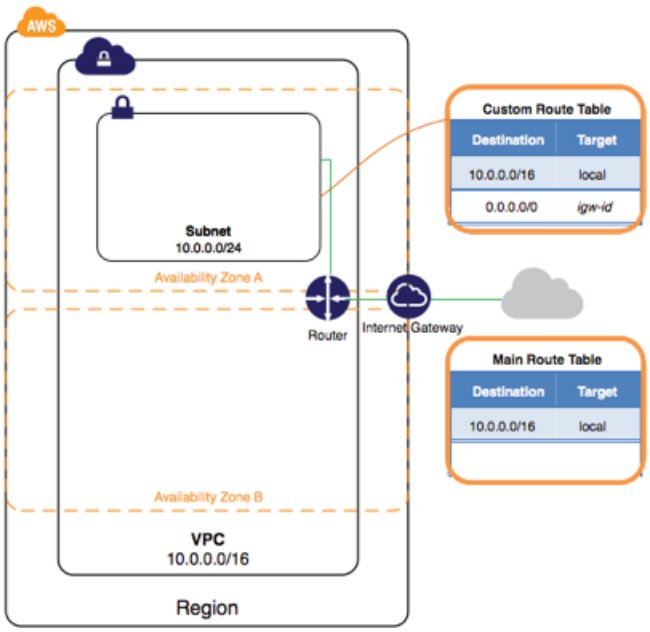
목차

1단계: VPC 생성

이 단계에서는 Amazon VPC 콘솔의 Amazon VPC 마법사를 사용하여 VPC를 생성합니다. 마법사는 다음 단계를 수행합니다.

- CIDR 블록이 /16인 VPC(프라이빗 IP 주소 65,536개를 가진 네트워크)를 생성합니다. VPC 크기 조정 및 CIDR 표기법에 대한 자세한 내용은 VPC 단원을 참조하십시오.
- 인터넷 게이트웨이를 VPC에 연결합니다. 인터넷 게이트웨이에 대한 자세한 내용은 인터넷 게이트웨이를 참조하십시오.
- VPC에 크기가 /24인 서브넷(프라이빗 IP 주소 256개 범위)을 생성합니다.
- 사용자 지정 라우팅 테이블을 만들고 서브넷에 연결하여 서브넷과 인터넷 게이트웨이 간에 트래픽이 전달될 수 있도록 합니다. 라우팅 테이블에 대한 자세한 내용은 라우팅 테이블 단원을 참조하십시오.

다음 다이어그램은 이 단계를 마친 후의 VPC 아키텍처를 보여 줍니다.

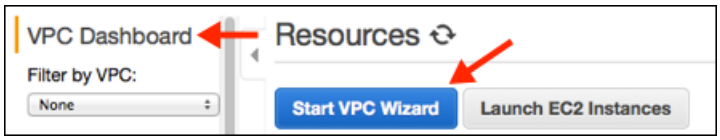


Note

이 연습에서는 VPC 마법사의 첫 번째 시나리오를 다룹니다. 다른 시나리오에 대한 자세한 내용은 Scenarios for Amazon VPC 단원을 참조하십시오.

Amazon VPC 마법사를 사용하여 VPC를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 오른쪽 상단의 탐색 모음에서 VPC를 생성하려는 리전을 기록해 둡니다. 다른 리전의 VPC에서 인스턴스를 시작할 수 없으므로 이 연습의 나머지 부분에서는 같은 리전에서 작업을 계속해야 합니다. 리전에 대한 자세한 내용은 리전 및 가용 영역을 참조하십시오.
3. Amazon VPC 대시보드에서 [Start VPC Wizard]를 선택합니다.

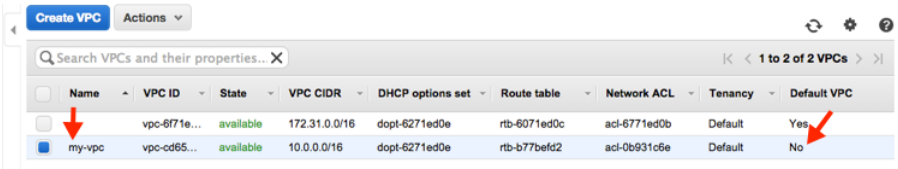


4. 첫 번째 옵션인 [VPC with a Single Public Subnet]을 선택한 후 [Select]를 선택합니다.
5. 구성 페이지에서 [VPC name] 필드에 VPC 이름을 입력합니다. 예를 들어, `my-vpc`를 입력하고 [Subnet name] 필드에 서브넷 이름을 입력합니다. 이렇게 하면 VPC와 서브넷을 만든 후 Amazon VPC 콘솔에서 이들을 식별하는 데 도움이 됩니다. 이 연습에서는 페이지 구성 설정의 나머지 부분을 그대로 두고 [Create VPC]를 선택합니다.

   (선택 사항) 원할 경우 구성 설정을 다음과 같이 수정한 다음 [Create VPC]를 선택합니다.

   - [IP CIDR block]에는 VPC(`10.0.0.0/16`)에 사용할 IP 주소 범위가 표시되고, [Public subnet] 필드에는 서브넷(`10.0.0.0/24`)에 사용할 IP 주소 범위가 표시됩니다. 기본 CIDR 범위를 사용하지 않으려는 경우 직접 지정할 수 있습니다. 자세한 내용은 VPC 크기 조정 및 서브넷 크기 조정을 참조하십시오.
   - 서브넷을 생성할 가용 영역은 [Availability Zone] 목록에서 선택할 수 있습니다. [No Preference]로 두면 AWS가 가용 영역을 선택합니다. 자세한 내용은 리전 및 가용 영역을 참조하십시오.
   - [Add endpoints for S3 to your subnets] 섹션에서 같은 리전의 Amazon S3에 VPC 엔드포인트를 생성할 서브넷을 선택할 수 있습니다. 자세한 내용은 VPC 엔드포인트를 참조하십시오.
   - [Enable DNS hostnames] 옵션을 [Yes]로 설정하면 VPC에서 시작되는 인스턴스가 DNS 호스트 이름을 수신합니다. 자세한 내용은 VPC에서 DNS 사용하기 섹션을 참조하십시오.
   - [Hardware tenancy] 옵션을 사용하면 VPC에서 시작되는 인스턴스가 공유 하드웨어에서 실행되는지 아니면 전용 하드웨어에서 실행되는지를 선택할 수 있습니다. 전용 테넌시를 선택하면 추가 비용이 발생합니다. 하드웨어 테넌시에 대한 자세한 내용은 전용 인스턴스 단원을 참조하십시오.

6. 상태 창에 진행 중인 작업이 표시됩니다. 작업이 끝나면 [OK]를 선택하여 상태 창을 닫습니다.
7. [Your VPCs] 페이지에 방금 생성했던 VPC 및 기본 VPC가 표시됩니다. 생성했던 VPC는 기본이 아닌 VPC이므로 [Default VPC] 열에 [No]라고 표시됩니다.



VPC에 대한 정보 보기

VPC를 생성했으면 서브넷, 인터넷 게이트웨이, 라우팅 테이블의 정보를 볼 수 있습니다. 생성한 VPC에는 두 개의 라우팅 테이블이 있습니다. 하나는 모든 VPC에 기본적으로 들어 있는 기본 라우팅 테이블이고 다른 하나는 마법사를 통해 생성한 사용자 지정 라우팅 테이블입니다. 사용자 지정 라우팅 테이블은 서브넷에 연결되어 있습니다. 즉, 이 테이블의 라우팅이 서브넷의 트래픽 흐름 방식을 결정합니다. VPC에 새 서브넷을 추가할 경우 기본값으로 기본 라우팅 테이블을 사용합니다.

VPC에 대한 정보 보기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Your VPCs]를 선택합니다. 생성한 VPC의 이름과 ID([Name] 및 [VPC ID] 열 확인)를 기록해 둡니다. 이 정보를 사용하여 VPC와 연결되는 구성 요소를 식별할 수 있습니다.

3. 탐색 창에서 [Subnets]를 선택합니다. VPC를 생성할 때 생성된 서브넷이 콘솔에 표시됩니다. 서브넷을 [Name] 열에서 이름으로 식별하거나, 전 단계에서 얻은 VPC 정보를 참조하여 [VPC] 열에서 살펴볼 수 있습니다.
4. 탐색 창에서 [Internet Gateways]를 선택합니다. [VPC] 열을 참조하여 VPC에 연결된 인터넷 게이트웨이를 확인할 수 있습니다. 이 열에는 VPC의 ID와 이름(해당하는 경우)이 표시됩니다.
5. 탐색 창에서 [Route Tables]를 선택합니다. VPC와 연결된 라우팅 테이블은 2개가 있습니다. 사용자 지정 라우팅 테이블([Main] 열에 [No]라고 표시됨)을 선택한 후 [Routes] 탭을 선택하여 세부 정보 창에서 라우팅 정보를 조회합니다.

   - 테이블의 첫 번째 행은 로컬 경로로 VPC 내에 있는 인스턴스의 통신을 가능하게 합니다. 이 라우팅은 기본적으로 모든 라우팅 테이블에 있으며 삭제할 수 없습니다.
   - 두 번째 행에는 VPC 외부의 IP 주소(`0.0.0.0/0`)로 향하는 트래픽이 서브넷에서 인터넷 게이트웨이로 전송될 수 있도록 하기 위해 Amazon VPC 마법사가 추가한 경로가 표시됩니다.

6. 기본 라우팅 테이블을 선택합니다. 기본 라우팅 테이블에는 로컬 경로만 있으며 그 외 다른 경로는 없습니다.

2단계: 보안 그룹 만들기

보안 그룹은 가상 방화벽 역할을 하여 관련 인스턴스에 대한 트래픽을 제어합니다. 보안 그룹을 사용하려면 인스턴스로 수신되는 트래픽을 제어할 인바운드 규칙과, 인스턴스에서 발신되는 트래픽을 제어하는 아웃바운드 규칙을 추가합니다. 보안 그룹을 인스턴스와 연결하려면 인스턴스를 시작할 때 보안 그룹을 지정합니다. 보안 그룹에 규칙을 추가 및 삭제할 경우 변경 사항은 보안 그룹과 관련된 인스턴스에 자동으로 적용됩니다.

VPC는 *기본 보안 그룹*과 함께 제공됩니다. 시작 시 별도의 보안 그룹과 연결되지 않은 모든 인스턴스는 기본 보안 그룹과 연결됩니다. 이 연습에서는 새로운 보안 그룹인 `WebServerSG`를 생성하고, VPC에서 인스턴스를 시작할 때 이 보안 그룹을 지정합니다.

Topics

WebServerSG 보안 그룹 규칙

다음 표에서는 `WebServerSG` 보안 그룹의 인바운드 규칙과 아웃바운드 규칙을 설명합니다. 인바운드 규칙은 직접 추가합니다. 아웃바운드 규칙은 모든 아웃바운드 통신을 허용하는 기본 규칙이므로, 이 규칙은 직접 추가할 필요가 없습니다.

인바운드			
소스 IP	프로토콜	포트 범위	설명
0.0.0.0/0	TCP	80	어디서든 인바운드 HTTP 액세스를 허용합니다.
0.0.0.0/0	TCP	443	어디서든 인바운드 HTTPS 액세스를 허용합니다.
홈 네트워크의 공인 IP 주소 범위	TCP	22	홈 네트워크에서 Linux/UNIX 인스턴스로의 인바운드 SSH 액세스를 허용합니다.

홈 네트워크의 공인 IP 주소 범위	TCP	3389	홈 네트워크에서 Windows 인스턴스로의 인바운드 RDP 액세스를 허용합니다.
아웃바운드			
목적지 IP	프로토콜	포트 범위	설명
0.0.0.0/0	모두	모두	모든 아웃바운드 통신을 허용하는 기본 아웃바운드 규칙입니다.

WebserverSG 보안 그룹 만들기

Amazon VPC 콘솔을 사용하여 보안 그룹을 만들 수 있습니다.

WebServerSG 보안 그룹을 만들어 규칙을 추가하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Security Groups]를 선택합니다.
3. [Create Security Group]을 선택합니다.
4. [Group name] 필드에 보안 그룹의 이름으로 `WebServerSG`를 입력하고 설명을 제공합니다. 필요에 따라 [Name tag] 필드를 사용하여 키가 `Name`인 보안 그룹에 대한 태그를 생성하거나 지정한 값을 사용할 수 있습니다.
5. [VPC] 메뉴에서 VPC ID를 선택한 다음 [Yes, Create]를 선택합니다.
6. 방금 생성한 `WebServerSG` 보안 그룹을 선택합니다. [Group Name] 열에서 이름을 볼 수 있습니다.
7. [Inbound Rules] 탭에서 [Edit]를 선택하고 다음과 같이 인바운드 트래픽에 대한 규칙을 추가한 후 완료되면 [Save]를 선택합니다.

   a. [Type] 목록에서 HTTP를 선택한 다음, `0.0.0.0/0`를 [Source] 필드에 입력합니다.

   b. [Add another rule]을 선택한 후 [Type] 목록에서 [HTTPS]를 선택하고 [Source] 필드에 `0.0.0.0/0`을 입력합니다.

   c. [Add another rule]을 선택합니다. Linux 인스턴스를 시작할 경우 [Type] 목록에서 [SSH]를 선택합니다. Windows 인스턴스를 시작할 경우에는 [Type] 목록에서 [RDP]를 선택합니다. 네트워크의 공인 IP 주소 범위를 Source(원본) 필드에 입력합니다. 주소 범위를 모르는 경우 이 연습에서 `0.0.0.0/0`을 사용할 수 있습니다.

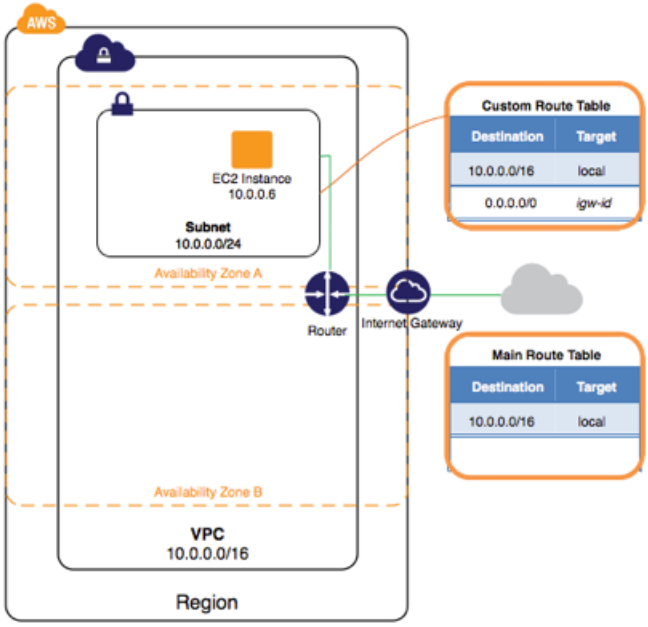
Caution

`0.0.0.0/0`을 사용하는 경우 모든 IP 주소에서 SSH 또는 RDP를 사용하여 인스턴스에 액세스할 수 있습니다. 따라서 연습에서는 잠시 사용해도 되지만 프로덕션 환경에서 사용하는 것은 안전하지 않습니다. 프로덕션에서는 특정 IP 주소나 주소 범위만 인스턴스에 액세스하도록 허용하십시오.

3단계: VPC에서 인스턴스 시작

VPC에서 EC2 인스턴스를 시작할 때 해당 인스턴스를 시작할 서브넷을 지정해야 합니다. 이 경우, 생성한 VPC의 퍼블릭 서브넷에서 인스턴스를 시작합니다. Amazon EC2 콘솔에서 Amazon EC2 시작 마법사를 사용하여 인스턴스를 시작합니다.

다음 다이어그램은 이 단계를 마친 후의 VPC 아키텍처를 보여 줍니다.



VPC에서 EC2 인스턴스를 시작하려면 다음을 수행합니다.

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 오른쪽 상단의 탐색 모음에서 VPC 및 보안 그룹을 생성했던 리전과 동일한 리전을 선택합니다.
3. 대시보드에서 [Launch Instance]를 선택합니다.
4. 마법사의 첫 페이지에서, 사용하려는 AMI를 선택합니다. 이 연습에서는 Amazon Linux AMI 또는 Windows AMI를 선택하는 것이 좋습니다.
5. [Choose an Instance Type] 페이지에서는 시작할 인스턴스의 하드웨어 구성과 크기를 선택할 수 있습니다. 마법사는 사용자가 선택한 AMI를 기반으로 하여 첫 번째로 사용 가능한 인스턴스 유형을 기본적으로 선택합니다. 기본 선택을 그대로 두고 [Next: Configure Instance Details]를 선택합니다.
6. [Configure Instance Details] 페이지의 [Network] 목록에서 생성한 VPC를 선택하고, [Subnet] 목록에서 서브넷을 선택합니다. 나머지 기본 설정을 그대로 두고 [Tag Instance] 페이지에 도달할 때까지 마법사의 다음 페이지로 이동합니다.
7. [Tag Instance] 페이지에서는 인스턴스에 `Name`을 사용하여 태그를 지정할 수 있습니다(예: `Name=MyWebServer`). 이렇게 하면 인스턴스를 시작한 후 Amazon EC2 콘솔에서 해당 인스턴스를 식별하는 데 도움이 됩니다. 모두 마쳤으면 [Next: Configure Security Group]을 선택합니다.
8. [Configure Security Group] 페이지에서 마법사는 사용자가 인스턴스에 연결할 수 있도록 마법사 시작 *x* 보안 그룹을 자동으로 정의합니다. 대신, [Select an existing security group] 옵션을 선택하고, 이전에 생성한 [WebServerSG] 그룹을 선택한 후 [Review and Launch]를 선택합니다.
9. [Review Instance Launch] 페이지에서 인스턴스의 세부 정보를 확인한 다음 [Launch]를 선택합니다.
10. Select an existing key pair or create a new key pair(기존 키 쌍 선택 또는 새 키 쌍 만들기) 대화 상자에서 기존 키 쌍을 선택하거나 새 키 쌍을 만들 수 있습니다. 새 키 페어를 만들 경우, 파일을 다운로드한 후 안전한 위치에 저장해야 합니다. 인스턴스를 실행한 후 인스턴스에 연결하려면 개인 키 콘텐츠가 필요합니다.

인스턴스를 시작하려면 승인 확인란을 선택한 후 [Launch Instances]를 선택합니다.

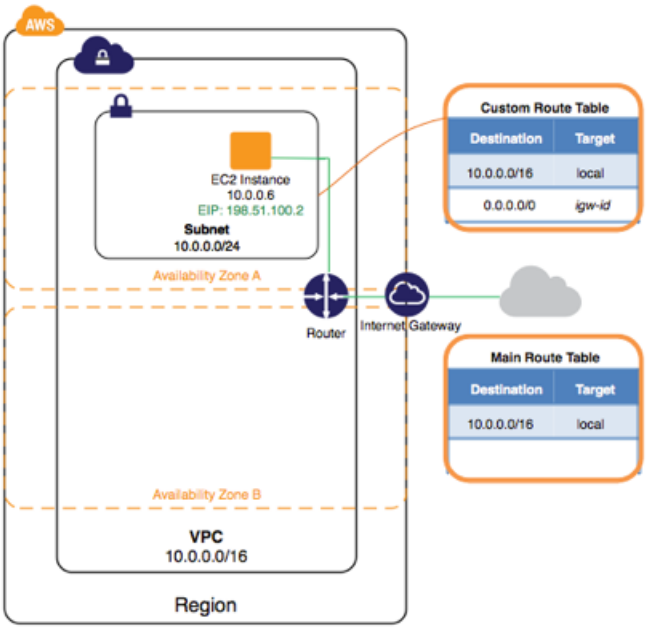
11. 확인 페이지에서 [View Instances]를 선택하여 [Instances] 페이지에서 해당 인스턴스를 확인합니다. 인스턴스를 선택하고 [Description] 탭에서 세부 정보를 확인합니다. [Private IPs] 필드에는 서브넷의 IP 주소 범위에서 인스턴스에 할당된 프라이빗 IP 주소가 표시됩니다.

Amazon EC2 시작 마법사에서 사용할 수 있는 옵션에 대한 자세한 내용은 *Linux 인스턴스용 Amazon EC2 사용 설명서*의 인스턴스 시작을 참조하십시오.

4단계: 인스턴스에 엘라스틱 IP 주소 할당

이전 단계에서, 인터넷 게이트웨이로 라우팅되는 서브넷인 퍼블릭 서브넷에서 인스턴스를 시작했습니다. 그러나 이 서브넷의 인스턴스는 인터넷과 통신할 수 있는 퍼블릭 IP 주소도 필요로 합니다. 기본이 아닌 VPC의 인스턴스는 기본적으로 퍼블릭 IP 주소가 지정되지 않습니다. 이 단계에서는 엘라스틱 IP 주소를 계정에 할당한 후 인스턴스와 연결합니다. 엘라스틱 IP 주소에 대한 자세한 정보는 엘라스틱 IP 주소를 참조하십시오.

다음 다이어그램은 이 단계를 마친 후의 VPC 아키텍처를 보여 줍니다.



엘라스틱 IP 주소를 할당 및 지정하려면 다음을 수행합니다.

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Elastic IPs]를 선택합니다.
3. [Allocate New Address]를 선택한 다음 [Yes, Allocate]를 선택합니다.

   Note

   해당 계정이 EC2-Classic을 지원할 경우, 우선 [Network platform] 목록에서 [EC2-VPC]를 선택합니다.

4. 목록에서 엘라스틱 IP 주소와 [Actions], [Associate Address]를 차례로 선택합니다.

5. 대화 상자의 [Associate with] 목록에서 [Instance]를 선택하고, [Instance] 목록에서 해당 인스턴스를 선택합니다. 작업을 마치면 [Yes, Associate]를 선택합니다.

이제 인스턴스를 인터넷에서 액세스할 수 있습니다. 또한 홈 네트워크에서 SSH 또는 원격 데스크톱을 사용하여 엘라스틱 IP 주소를 통해 인스턴스에 연결할 수 있습니다. Linux 인스턴스에 연결하는 방법에 대한 자세한 내용은 *Linux 인스턴스용 Amazon EC2 사용 설명서*의 [Connecting to Your Linux Instance]를 참조하십시오. Windows 인스턴스에 연결하는 방법에 대한 자세한 내용은 *Microsoft Windows 인스턴스용 Amazon EC2 사용 설명서*의 [Connect to Your Windows Instance Using RDP]를 참조하십시오.

이것으로 연습을 마쳤습니다. 이제 VPC에서 인스턴스를 계속 사용하거나, 인스턴스가 더 이상 필요하지 않을 경우 인스턴스를 종료하고 엘라스틱 IP 주소를 릴리스하여 비용이 발생하지 않도록 할 수 있습니다. VPC를 삭제할 수도 있습니다. 단, 서브넷과 라우팅 테이블 등 이 연습에서 만든 VPC 구성 요소 및 VPC에 대해서는 요금이 청구되지 않습니다.

5단계: 정리

VPC를 삭제하기 전에 VPC 내에 실행하고 있는 모든 인스턴스를 종료해야 합니다. VPC 콘솔을 사용하여 VPC를 삭제하면 서브넷, 보안 그룹, 네트워크 ACL, DHCP 옵션 세트, 라우팅 테이블, 인터넷 게이트웨이 등 VPC와 관련된 리소스 또한 삭제됩니다.

인스턴스를 종료하려면 엘라스틱 IP 주소를 릴리스하고 VPC를 삭제하십시오.

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Instances]를 선택합니다.
3. 인스턴스를 선택하고 [Actions]를 선택한 후 [Instance State]와 [Terminate]를 차례로 선택합니다.
4. 대화 상자에서 [Release attached Elastic IPs] 섹션을 확장하고 엘라스틱 IP 주소 옆에 있는 확인란을 선택합니다. [Yes, Terminate]를 선택합니다.
5. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
6. 탐색 창에서 [Your VPCs]를 선택합니다.
7. VPC를 선택하고 [Actions]를 선택한 후 [Delete VPC]를 선택합니다.
8. 확인 메시지가 나타나면 [Yes, Delete]를 선택합니다.