배스천 호스트를 사용하여 원격 인스턴스에 안전하게 액세스

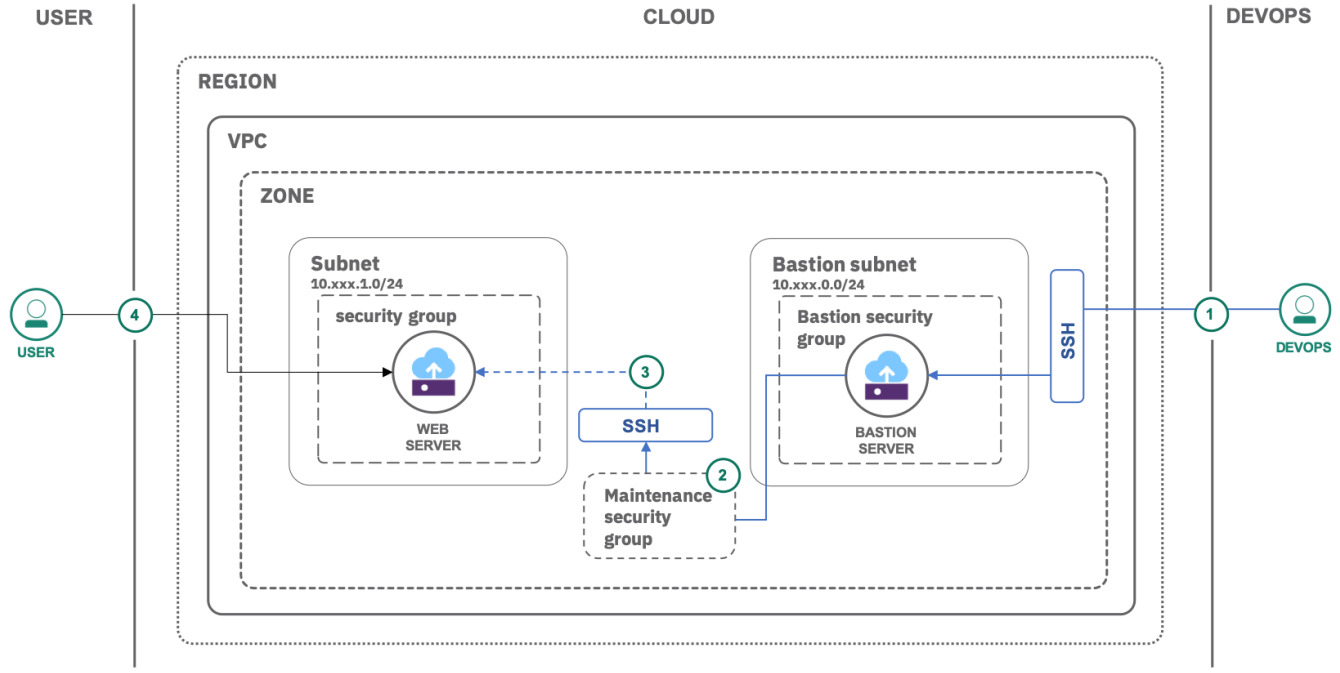
비용 추정치를 생성하십시오.

이 튜토리얼에서는 가상 프라이빗 클라우드 내에서 원격 인스턴스에 안전하게 액세스하기 위한 배스천 호스트의 배치에 대해 설명합니다. 배스천 호스트(bastion host)는 공인 IP 주소로 프로비저닝되고 SSH를 통해 액세스될 수 있는 인스턴스입니다. 설정되고 나면 배스천 호스트는 **점프** 서버 역할을 수행하여 공인 IP 주소 없이 프로비저닝된 인스턴스에 대한 보안 연결을 허용합니다.

VPC 내에서 서버 노출을 줄이기 위해 배스천 호스트를 작성하고 사용합니다. 개별 서버에 대한 관리 태스크는 배스천을 통해 프록시로 전송되어 SSH를 사용하여 수행됩니다. 서버에 대한 액세스 및 서버로부터의 일반 인터넷 액세스(예: 소프트웨어 설치의 경우)는 해당 서버에 접속된 특수 유지보수 보안 그룹에만 허용됩니다.

목표

- 배스천 호스트 및 규칙이 있는 보안 그룹을 설정하는 방법을 학습합니다.
- 배스천 호스트를 통해 서버를 안전하게 관리합니다.



1. 클라우드에서 필수 인프라(서브넷, 규칙이 있는 보안 그룹, VSI)를 설정한 후 관리자(DevOps)가 개인용 SSH 키를 사용하여 배스천 호스트에 SSH를 통해 연결합니다.
2. 관리자가 적절한 아웃바운드 규칙을 가진 유지보수 보안 그룹을 지정합니다.
3. 관리자가 배스천 호스트를 통해 인스턴스의 사설 IP 주소에 SSH를 통해 안전하게 연결하여 필수 소프트웨어(예: 웹 서버)를 설치하거나 업데이트합니다.
4. 인터넷 사용자가 웹 서버에 대한 HTTP/HTTPS 요청을 작성합니다.

있는지 확인하십시오. 1세대용 VPC 또는 2세대용 VPC의 필수 권한 목록을 참조하십시오.

- 가상 서버에 연결하기 위해 SSH 키가 필요합니다. SSH 키가 없으면 1세대용 VPC 또는 2세대용 VPC의 키를 작성하기 위한 지시사항을 확인하십시오.
- 이 튜토리얼에서는 기존 가상 프라이빗 클라우드에서 배스천 호스트를 추가한다고 가정합니다. **계정에 가상 프라이빗 클라우드가 없는 경우에는 다음 단계로 진행하기 전에 가상 프라이빗 클라우드를 작성하십시오.**

단계 1: 배스천 호스트 작성

이 절에서는 별도의 서브넷에서 보안 그룹과 함께 배스천 호스트를 작성하고 구성합니다.

서브넷 작성

1. 왼쪽 분할창의 **네트워크** 아래에 있는 **서브넷**을 클릭한 후 **새 서브넷**을 클릭하십시오.
   - **vpc-secure-bastion-subnet**을 이름으로 입력한 후 작성된 VPC를 선택하십시오.
   - 위치 및 구역을 선택하십시오.
   - CIDR 표기법으로 서브넷의 IP 범위를 입력하십시오(예: **10.xxx.0.0/24**). **주소 접두부**는 그대로 두고 **주소 수**를 256으로 선택하십시오.

     참고: 1세대용 VPC를 사용하는 경우 서브넷 액세스 제어 목록(ACL)의 **VPC 기본값**을 선택하십시오. 나중에 인바운드 및 아웃바운드 규칙을 구성할 수 있습니다.

2. **퍼블릭 게이트웨이**를 **접속됨**으로 전환하십시오.

   팁: 퍼블릭 게이트웨이를 서브넷에 접속하면 접속된 모든 리소스가 공용 인터넷과 통신할 수 있습니다.

3. **서브넷 작성**을 클릭하여 이를 프로비저닝하십시오.

배스천 보안 그룹 작성 및 구성

보안 그룹을 작성하고 배스천 VSI에 대한 인바운드 규칙을 구성해 봅니다.

1. **보안 그룹**으로 이동한 후 **새 보안 그룹**을 클릭하십시오. **vpc-secure-bastion-sg**를 이름으로 입력한 후 VPC를 선택하십시오.
2. 이제 인바운드 섹션에서 **규칙 추가**를 클릭하여 다음과 같은 인바운드 규칙을 작성하십시오. 이 규칙은

주소를 확보하여 이를 대신 사용할 수 있습니다.

③ **보안 그룹 작성**을 클릭하여 작성하십시오.

프로토콜	소스 유형	소스	값
TCP	임의	0.0.0.0/0	포트 22-22
ICMP	임의	0.0.0.0/0	유형: **8**, 코드: **공백으로 둠**

배스천: 인바운드 규칙

배스천 인스턴스 작성

서브넷 및 보안 그룹이 이미 준비된 경우 다음으로 배스천 가상 서버 인스턴스를 작성하십시오.

① 왼쪽 분할창의 **서브넷** 아래에서 **vpc-secure-bastion-subnet**을 선택하십시오.

② **접속된 리소스**를 클릭한 후 자체 VPC 아래에서 **vpc-secure-bastion-vsi**라는 **새 인스턴스**를 프로비저닝하십시오.

③ **위치**를 선택한 후 나중에 동일한 위치를 다시 사용해야 합니다.

④ **컴퓨팅**(2 vCPU 및 4GB RAM)을 프로파일로 선택하십시오.

⑤ 새 **SSH 키**를 작성하려면 **새 키**를 클릭하십시오.

- **vpc-ssh-key**를 키 이름으로 입력하십시오.
- **지역**은 그대로 두십시오.
- 기존 로컬 SSH 키의 컨텐츠를 복사하여 **공개 키** 아래에 붙여넣으십시오.
- **SSH 키 추가**를 클릭하십시오.

⑥ **Ubuntu Linux**를 이미지로 선택하십시오. 이미지의 임의의 버전을 선택할 수 있습니다.

⑦ **네트워크 인터페이스** 아래에서 보안 그룹 옆의 **편집** 아이콘을 클릭하십시오.

- **vpc-secure-bastion-subnet**이 서브넷으로 선택되어 있는지 확인하십시오.
- 기본 보안 그룹을 선택 취소한 후 **vpc-secure-bastion-sg**를 선택하십시오.
- **저장**을 클릭하십시오.

⑧ **가상 서버 인스턴스 작성**을 클릭하십시오.

⑨ 인스턴스가 작성되면 **vpc-secure-bastion-vsi**를 클릭하고 유동 IP를 **예약**하십시오.

배스천 테스트

단계 2: 유지보수 액세스 규칙이 있는 보안 그룹 구성

배스천에 대한 액세스가 작동 중이면 계속하여 소프트웨어 설치 및 업데이트 등의 유지보수 태스크를 위해 보안 그룹을 작성하십시오.

1. **보안 그룹**으로 이동한 후 아래 표에 표시된 아웃바운드 규칙을 포함하는, **vpc-secure-maintenance-sg** 라는 새 보안 그룹을 프로비저닝하십시오.

   팁: DNS 서버 요청은 포트 53에서 주소가 지정됩니다. DNS는 구역 전송을 위해 TCP를 사용하고 이름 조회(일반(기본) 또는 예약)를 위해 UDP를 사용합니다. HTTP 요청은 포트 80 및 443에 있습니다.

2. 다음으로 아래 표에 표시된 **인바운드** 규칙을 추가하십시오. 이는 배스천 호스트에서의 SSH 액세스를 허용합니다.

3. 보안 그룹을 작성하십시오.

프로토콜	대상 유형	대상	값
TCP	임의	0.0.0.0/0	포트 80-80
TCP	임의	0.0.0.0/0	포트 443-443
TCP	임의	0.0.0.0/0	포트 53-53
UDP	임의	0.0.0.0/0	포트 53-53

유지보수: 아웃바운드 규칙

프로토콜	소스 유형	소스	값
TCP	보안 그룹	vpc-secure-bastion-sg	포트 22-22

유지보수: 인바운드 규칙

1. **보안 그룹**으로 이동한 후 **vpc-secure-bastion-sg**를 선택하십시오.

TCP	보안 그룹	vpc-secure-maintenance-sg	포트 22-22

배스천: 아웃바운드 규칙

단계 3: 배스천 호스트를 사용하여 VPC의 다른 인스턴스에 액세스

이 절에서는 보안 그룹 및 가상 서버 인스턴스가 있는 서브넷을 작성합니다.

연결하려는 가상 서버 인스턴스가 이미 VPC에 있는 경우에는 다음 세 개의 절을 건너뛰고 유지보수 보안 그룹에 가상 서버 인스턴스를 추가할 수 있습니다.

서브넷 작성

새 서브넷을 작성하려면 다음을 수행하십시오.

1. 왼쪽 분할창의 **네트워크** 아래에 있는 **서브넷**을 클릭한 후 **새 서브넷**을 클릭하십시오.
   - **vpc-secure-private-subnet**을 이름으로 입력한 후 작성된 VPC를 선택하십시오.
   - 위치를 선택하십시오.
   - CIDR 표기법으로 서브넷의 IP 범위를 입력하십시오(예: **10.xxx.1.0/24**). **주소 접두부**는 그대로 두고 **주소 수**를 256으로 선택하십시오.

     참고: 1세대용 VPC를 사용하는 경우 서브넷 액세스 제어 목록(ACL)의 **VPC 기본값**을 선택하십시오. 나중에 인바운드 및 아웃바운드 규칙을 구성할 수 있습니다.

2. **퍼블릭 게이트웨이**를 **접속됨**으로 전환하십시오.
3. **서브넷 작성**을 클릭하여 이를 프로비저닝하십시오.

보안 그룹 작성

새 보안 그룹을 작성하려면 다음을 수행하십시오.

1. 네트워크 아래에서 **보안 그룹**을 클릭한 후 **새 보안 그룹**을 클릭하십시오.
2. **vpc-secure-private-sg**를 이름으로 입력한 후 이전에 작성한 VPC를 선택하십시오.
3. **보안 그룹 작성**을 클릭하십시오.

가상 서버 인스턴스 작성

3. 고유 이름(**vpc-secure-private-vsi**)을 입력하고 이전에 작성한 VPC 및 리소스 그룹을 선택하십시오.
4. bastion Virtual Server에서 이미 사용한 이름과 같은 **위치**를 선택하십시오.
5. **컴퓨팅**(2 vCPU 및 4GB RAM)을 프로파일로 선택하십시오. 기타 사용 가능한 프로파일을 확인하고 **모든 프로파일**을 클릭하십시오.
6. **SSH 키**에 대해 배스천에 대해 이전에 작성한 SSH 키를 선택하십시오.
7. **Ubuntu Linux**를 이미지로 선택하십시오. 이미지의 임의의 버전을 선택할 수 있습니다.
8. **네트워크 인터페이스** 아래에서 보안 그룹 옆의 **편집** 아이콘을 클릭하십시오.
   - **vpc-secure-private-subnet**을 서브넷으로 선택하십시오.
   - 기본 보안 그룹을 선택 취소한 후 **vpc-secure-private-sg**를 활성화하십시오.
   - **저장**을 클릭하십시오.
9. **가상 서버 인스턴스 작성**을 클릭하십시오.

유지보수 보안 그룹에 가상 서버 추가

서버에서 관리 작업을 수행하려면 특정 가상 서버를 유지보수 보안 그룹과 연관시켜야 합니다. 다음에서는 유지보수를 사용으로 설정하고 개인용 서버에 로그인하고 소프트웨어 패키지 정보를 업데이트한 후 다시 보안 그룹의 연관을 해제합니다.

서버에 대해 유지보수 보안 그룹을 사용으로 설정해 봅니다.

1. **보안 그룹**으로 이동한 후 **vpc-secure-maintenance-sg** 보안 그룹을 선택하십시오.
2. **접속된 인터페이스**를 클릭한 후 **인터페이스 편집**을 클릭하십시오.
3. 가상 서버 인스턴스를 펼친 후 **인터페이스** 열에서 **기본** 옆의 선택을 활성화하십시오.
4. **저장**을 클릭하여 변경사항을 적용하십시오.

인스턴스에 연결

사설 IP를 사용하여 인스턴스에 SSH를 통해 접속하기 위해 배스천 호스트를 **점프 호스트**로 사용합니다.

1. **가상 서버 인스턴스** 아래에서 가상 서버 인스턴스의 사설 IP 주소를 확보하십시오.

2. ssh 명령을 `-J`와 함께 사용하여 **네트워크 인터페이스** 아래에 표시된 서버 **사설 IP** 주소 및 이전에 사용한 배스천 **유동 IP** 주소를 가진 서버에 로그인하십시오.

```
ssh -J root@<BASTION_FLOATING_IP_ADDRESS>
root@<PRIVATE_IP_ADDRESS>
```

소프트웨어 설치 및 유지보수 태스크 수행

연결되면 가상 서버에 소프트웨어를 설치하거나 유지보수 태스크를 수행할 수 있습니다.

1. 먼저 소프트웨어 패키지 정보를 업데이트하십시오.

```
$ apt-get update
```

2. 원하는 소프트웨어(예: Nginx, MySQL 또는 IBM Db2)를 설치하십시오.

완료되면 `exit` 명령을 사용하여 서버와의 연결을 끊으십시오.

> **팁:** 인터넷 사용자로부터의 HTTP/HTTPS 요청을 허용하려면 **유동 IP**를 VSI에 지정하고 개인용 VSI의 보안 그룹에 있는 인바운드 규칙을 통해 필수 포트(80 - HTTP 및 443 - HTTPS)를 여십시오.

유지보수 보안 그룹 사용 안함

소프트웨어 설치 또는 유지보수 수행이 완료되면 가상 서버를 유지보수 보안 그룹에서 제거하여 격리된 상태를 유지해야 합니다.

1. **보안 그룹**으로 이동한 후 **vpc-secure-maintenance-sg** 보안 그룹을 선택하십시오.
2. **접속된 인터페이스**를 클릭한 후 **인터페이스 편집**을 클릭하십시오.
3. 가상 서버 인스턴스를 펼친 후 **인터페이스** 열에서 **기본** 옆의 선택을 선택 취소하십시오.
4. **저장**을 클릭하여 변경사항을 적용하십시오.

단계 4: 리소스 제거

1. **Virtual Server 인스턴스**로 전환한 후 인스턴스를 **중지**하고 **삭제**하십시오.
2. VSI가 삭제되면 **서브넷**으로 전환한 후 서브넷을 삭제하십시오.
3. 서브넷이 삭제된 후 **가상 프라이빗 클라우드** 탭으로 전환하고 VPC를 삭제하십시오.

> **팁:** 콘솔 사용 시 리소스 삭제 후 업데이트된 상태 정보를 보려면 브라우저를 새로 고쳐야 할 수 있습니다.

관련 컨텐츠

public-app-private-backend)

How helpful was this tutorial?

1 2 3 4 5 6 7 8 9 10

< Not at all Worked great! >

언어:

한국어