한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. Challenge Lab 04

LAB 02. 네트워크 보안 그룹 구성

이 문서는 Microsoft Technical Trainer팀에서 ESI 교육 참석자분들에게 제공해 드리는 문서입니다.

Microsoft Partner Program – Technical Advisory Service

Microsoft

요약

이 내용들은 표시된 날짜에 Microsoft에서 검토된 내용을 바탕으로 하고 있습니다. 따라서, 표기된 날짜 이후에 시장의 요구사항에 따라 달라질 수 있습니다. 이 문서는 고객에 대한 표기된 날짜 이후에 변화가 없다는 것을 보증하지 않습니다.

이 문서는 정보 제공을 목적으로 하며 어떠한 보증을 하지는 않습니다.

문서 작성 연혁

날짜	버전	작성자	변경 내용
2023.08.27	1.0.0	우진환	LAB 02 내용 작성

목차

도전 과제

이 실습에서는 가상 머신에 대한 SSH 연결을 허용하도록 네트워크 보안 그룹을 구성합니다.

- 애플리케이션 보안 그룹을 만든 다음 네트워크 보안 그룹을 만듭니다.
- 네트워크 보안 그룹을 가상 네트워크의 서브넷에 연결한 다음 애플리케이션 보안 그룹을 가상 머신의 네트워크 인터페이스에 연결합니다.
- 인바운드 보안 규칙을 추가한 다음 SSH를 사용하여 서브넷의 가상 머신에 연결할 수 있는지 확인합니다.

STEP 01. Azure 보안 그룹 만들기

1. `RG1lod<xxxxxxxx>` 리소스 그룹에 `webapp201-asg` 이름의 애플리케이션 보안 그룹을 만듭니다.
2. `RG1lod<xxxxxxxx>` 리소스 그룹에 `webapp201-nsg` 이름의 네트워크 보안 그룹을 만듭니다.

STEP 02. Azure 보안 그룹을 Azure 리소스에 연결

1. `webapp201-nsg` 네트워크 보안 그룹을 `VNET` 가상 네트워크의 `frontend` 서브넷에 연결합니다.
2. `webapp201-asg` 애플리케이션 보안 그룹을 `VM1` 가상 머신의 네트워크 인터페이스에 연결합니다.

STEP 03. SSH를 사용하여 Linux 가상 머신에 연결

1. 다음 속성을 사용하여 [Cloud Shell]의 Bash 세션을 시작합니다.

속성	값
Cloud Shell 지역	미국 동부
리소스 그룹	rg1lod<xxxxxxxx>
스토리지 계정	sa<xxxxxxxx>
파일 공유	cloud-shell-share

2. [Cloud Shell]의 Bash 세션에서 `VM1` 가상 머신에 SSH 연결을 설정합니다.

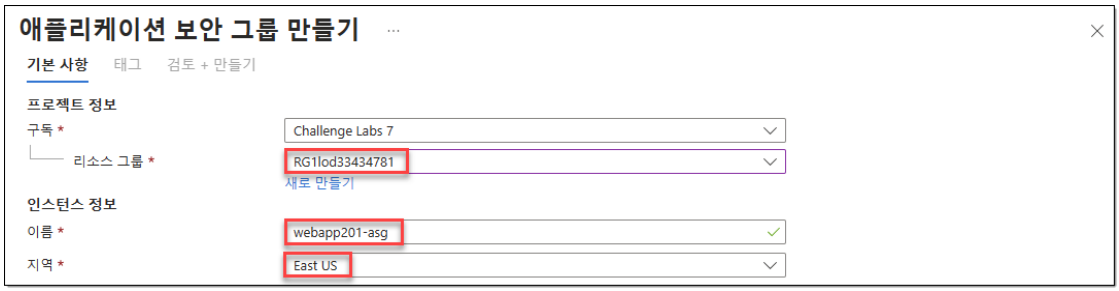
STEP 04. SSH를 허용하는 인바운드 보안 규칙 만들기

1. `webapp201-nsg` 네트워크 보안 그룹에 `TCP 22` 포트를 허용하는 "`AllowSSH`" 이름의 인바운드 보안 규칙을 추가합니다.
2. [Cloud Shell]의 Bash 세션에서 `VM1` 가상 머신에 SSH 연결이 되는지 확인합니다.

TASK 01. Azure 보안 그룹 만들기

1. Azure 포털의 검색창에서 "애플리케이션 보안 그룹"을 검색한 후 클릭합니다. [애플리케이션 보안 그룹] 블레이드의 메뉴에서 [만들기]를 클릭합니다.

2. [애플리케이션 보안 그룹 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: RG1lod<xxxxxxxx>
   - [인스턴스 정보 - 이름]: webapp201-asg
   - [인스턴스 정보 - 지역]: East US

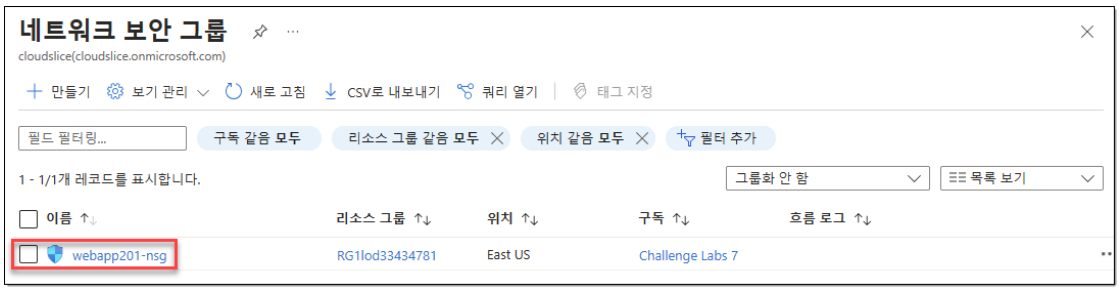


3. 네트워크 트래픽을 필터링하는데 사용할 수 있는 두 가지 유형의 Azure 보안 그룹이 있습니다.
   - 애플리케이션 보안 그룹을 사용하여 유사한 워크로드를 실행하는 Azure 가상 머신을 그룹화합니다.
   - 네트워크 보안 그룹을 사용하여 소스, 소스 포트, 대상, 대상 포트 및 프로토콜을 기반으로 네트워크 트래픽을 허용하거나 거부하는데 사용하는 규칙을 정의합니다.
   - 애플리케이션 보안 그룹에서는 동일한 서브넷에 여러 애플리케이션을 배포할 수 있지만 애플리케이션을 서로 격리된 상태로 유지할 수 있습니다.
   - 네트워크 보안 그룹에서는 애플리케이션 보안 그룹을 기반으로 하는 네트워크 보안 정책을 정의할 수 있습니다. 이를 통해 명시적인 IP 주소가 아닌 워크로드를 기반으로 해당 정책을 정의할 수 있습니다.
4. Azure 포털의 검색창에서 "네트워크 보안 그룹"을 검색한 후 클릭합니다. [네트워크 보안 그룹] 블레이드의 메뉴에서 [만들기]를 클릭합니다.

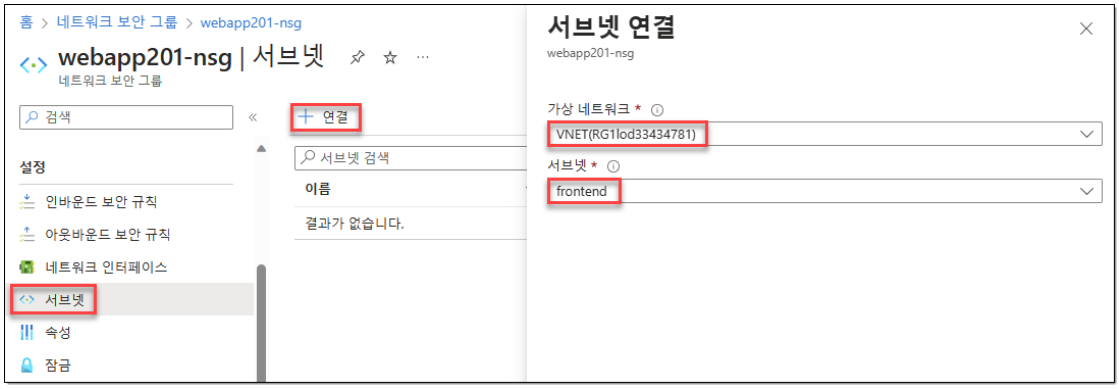
5. [네트워크 보안 그룹 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: `RG1lod<xxxxxxxx>`
   - [인스턴스 정보 - 이름]: webapp201-nsg
   - [인스턴스 정보 - 지역]: East US

TASK 02. Azure 보안 그룹을 Azure 리소스에 연결

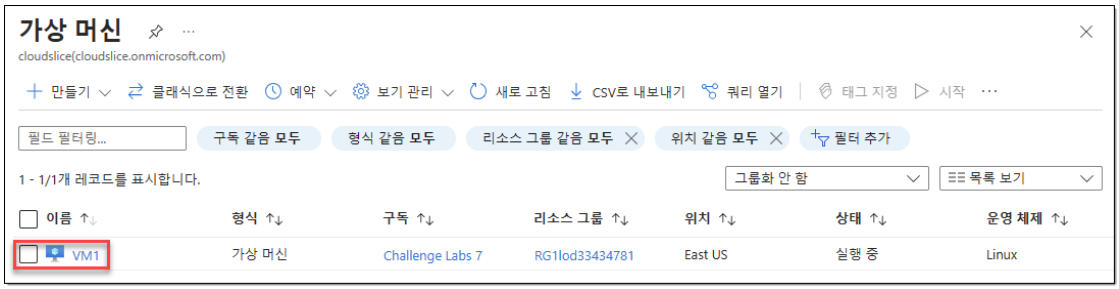
1. [네트워크 보안 그룹] 블레이드에서 앞서 만들었던 `webapp201-nsg` 네트워크 보안 그룹을 클릭합니다.



2. [`webapp201-nsg` 네트워크 보안 그룹] 블레이드의 [설정 - 서브넷]으로 이동한 후 메뉴에서 [연결]을 클릭합니다. [서브넷 연결] 창에서 아래와 같이 구성한 후 [확인]을 클릭합니다.
   - 가상 네트워크: `VNET(RG1lod<xxxxxxxx>)`
   - 서브넷: frontend

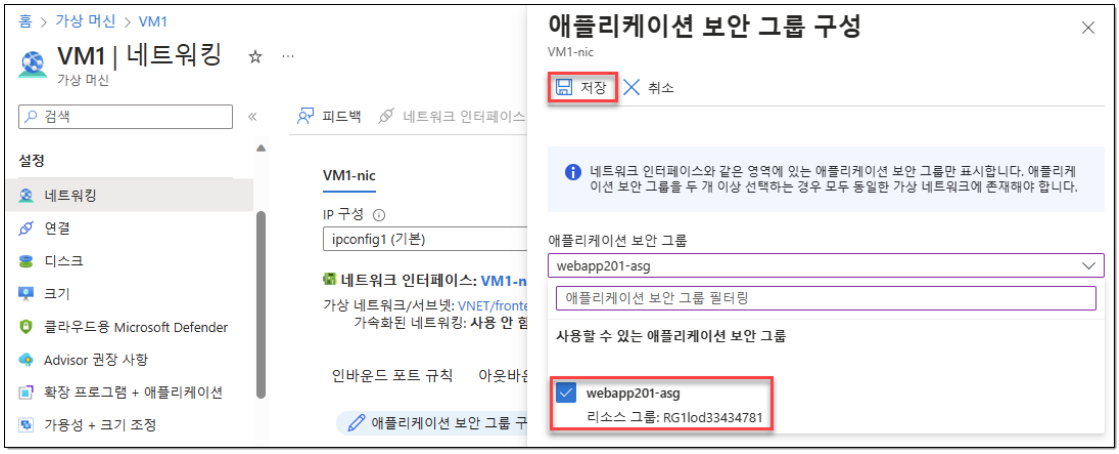


3. 네트워크 보안 그룹은 가상 머신의 NIC이나 애플리케이션 보안 그룹과 동일한 지역에 있는 서브넷에 연결할 수 있습니다. 커뮤니케이션에 문제를 일으킬 수 있는 규칙 충돌을 방지하려면 네트워크 보안 그룹을 서브넷이나 NIC 중 하나에만 연결해야 하며 둘 다에 연결하지 않는 것이 좋습니다.
4. Azure 포털의 검색창에서 "가상 머신"을 검색한 후 클릭합니다. [가상 머신] 블레이드에서 `VM1` 가상 머신을 클릭합니다.



5. [`VM1` 가상 머신] 블레이드의 [설정 - 네트워킹]으로 이동합니다. [애플리케이션 보안 그룹] 탭에서 [애플리케이션 보안 그룹 구성]을 클릭합니다.

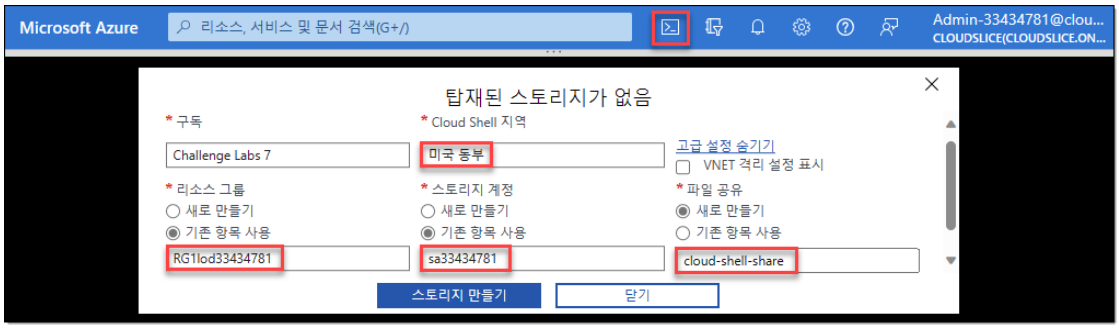
6. [애플리케이션 보안 그룹 구성] 창에서 "`webapp201-asg`" 애플리케이션 보안 그룹을 선택한 후 [저장]을 클릭합니다.



7. [VM1 가상 머신] 블레이드의 [개요]로 이동한 후 공용 IP 주소를 메모장에 기록합니다.

TASK 03. SSH를 사용하여 Linux 가상 머신에 연결

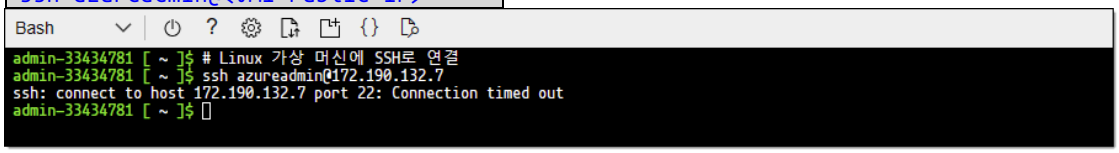
1. Azure 포털에서 [Cloud Shell]을 클릭한 후 "Bash"를 선택합니다. [탑재된 스토리지가 없음] 창에서 "고급 설정 표시"를 클릭합니다. [탑재된 스토리지가 없음] 페이지에서 아래와 같이 구성한 후 [스토리지 만들기]를 클릭합니다.
   - Cloud Shell 지역: 미국 동부
   - 리소스 그룹: "기존 항목 사용"을 선택한 후 "RG1lod<xxxxxxxxx>" 리소스 그룹을 선택합니다.
   - 스토리지 계정: "기존 항목 사용"을 선택한 후 "sa<xxxxxxxxx>" 스토리지 계정을 선택합니다.
   - 파일 공유: "새로 만들기"를 선택한 후 "cloud-shell-share" 이름을 입력합니다.



2. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 VM1 가상 머신에 SSH 세션을 연결합니다. 네트워크 보안 그룹에서 SSH 세션을 허용하도록 설정하지 않았기 때문에 연결 제한 시간 초과가

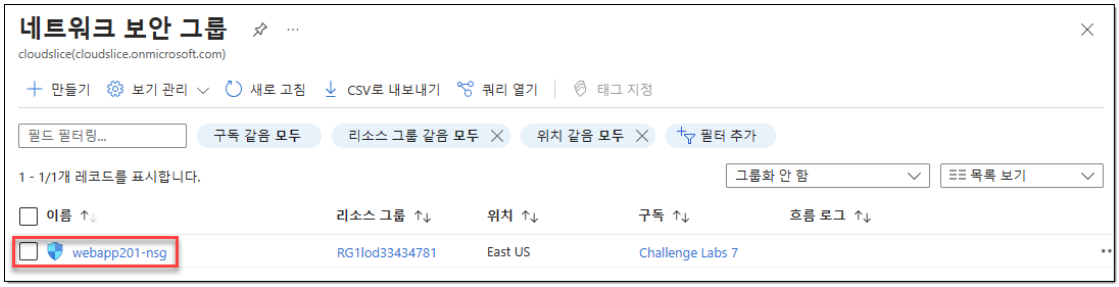
발생하는 것을 확인합니다.

```
# Linux 가상 머신에 SSH 로 연결
ssh azureadmin@<VM1 Public IP>
```

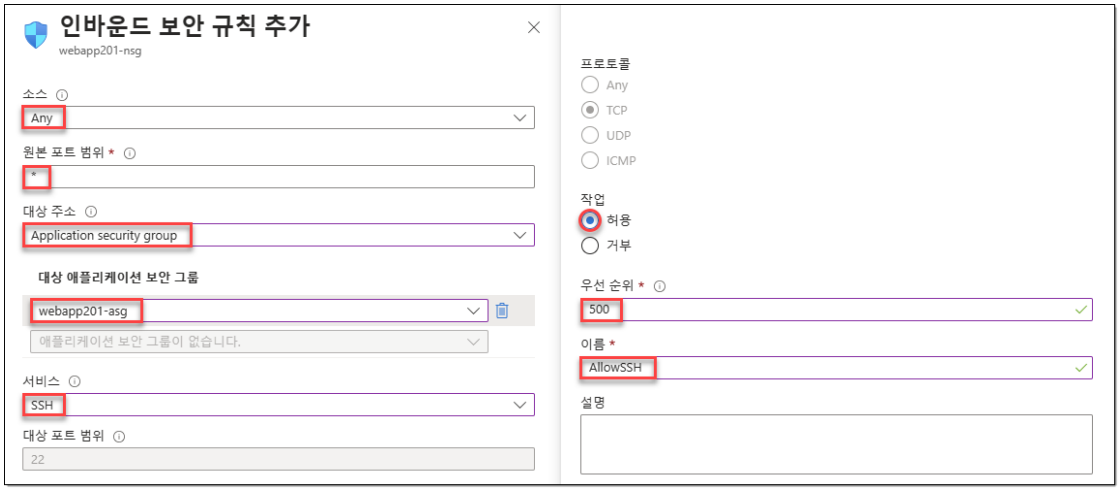


TASK 04. SSH를 허용하는 인바운드 보안 규칙 만들기

1. Azure 포털의 검색창에서 "네트워크 보안 그룹"을 검색한 후 클릭합니다. [네트워크 보안 그룹] 블레이드에서 `webapp201-nsg` 네트워크 보안 그룹을 클릭합니다.

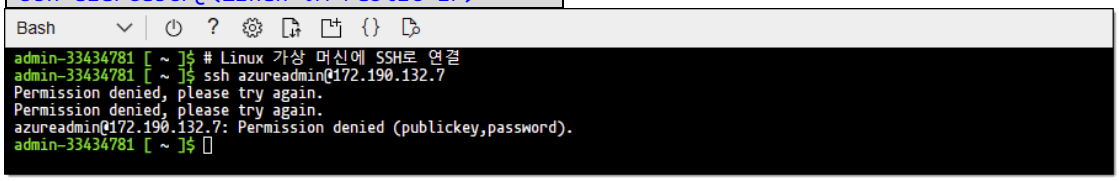


2. [`webapp201-nsg` 네트워크 보안 그룹] 블레이드의 [설정 - 인바운드 보안 규칙]으로 이동한 후 메뉴에서 [추가]를 클릭합니다. [인바운드 보안 규칙 추가] 창에서 아래와 같이 구성한 후 [추가]를 클릭합니다.
   - 소스: Any
   - 원본 포트 범위: *
   - 대상 주소: Application security group
   - 대상 애플리케이션 보안 그룹: webapp201-app
   - 서비스: SSH
   - 작업: 허용
   - 우선 순위: 500
   - 이름: AllowSSH



3. [Cloud Shell]의 Bash 세션을 다시 열고 다음 명령을 실행하여 `VM1`에 대한 SSH 연결을 시도합니다. Bash 세션에서 아래와 같이 권한 오류가 발생하면 자신의 컴퓨터에서 터미널을 실행하여 동일한 작업을 진행합니다.

```
# Linux 가상 머신에 SSH 로 연결
ssh azureuser@<Linux VM Public IP>
```



4. 자신의 컴퓨터에서 [터미널]을 열고 동일한 명령을 실행합니다. 아래와 같이 `VM1` 가상 머신에 연결되는 것을 확인합니다.

```
# Linux 가상 머신에 SSH 로 연결
ssh azureuser@<Linux VM Public IP>
```