

AZ-104. Challenge Lab 04

## **LAB 03. 가상 네트워크에서 경로 테이블 구성**

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

**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.

저작권에 관련된 법률을 준수하는 것은 고객의 역할이며, 이 문서를 마이크로소프트의 사전 동의 없이 어떤 형태(전자 문서, 물리적인 형태 막론하고) 어떠한 목적으로 재 생산, 저장 및 다시 전달하는 것은 허용되지 않습니다.

마이크로소프트는 이 문서에 들어있는 특허권, 상표, 저작권, 지적 재산권을 가집니다. 문서를 통해 명시적으로 허가된 경우가 아니면, 어떠한 경우에도 특허권, 상표, 저작권 및 지적 재산권은 다른 사용자에게 허용되지 않습니다.

© 2023 Microsoft Corporation All right reserved.

Microsoft®는 미합중국 및 여러 나라에 등록된 상표입니다.

이 문서에 기재된 실제 회사 이름 및 제품 이름은 각 소유자의 상표일 수 있습니다.

## 문서 작성 연혁

날짜	버전	작성자	변경 내용
2023.08.27	1.0.0	우진환	LAB 03 내용 작성

## 목차

<b>도전 과제</b> .....	<b>5</b>
STEP 01. 기존 가상 머신의 IP 확인 .....	5
STEP 02. 프런트 엔드 경로 테이블 구성.....	5
STEP 03. 백 엔드 경로 테이블 구성 .....	5
STEP 04. 가상 어플라이언스에 IP 전달 구성 .....	5
STEP 05. TRACEROUTE 도구를 사용하여 경로 테스트 .....	6
<b>TASK 01. 기존 가상 머신의 IP 확인</b> .....	<b>7</b>
<b>TASK 02. 프런트 엔드 경로 테이블 구성</b> .....	<b>7</b>
<b>TASK 03. 백 엔드 경로 테이블 구성</b> .....	<b>9</b>
<b>TASK 04. 가상 어플라이언스에 IP 전달 구성</b> .....	<b>11</b>
<b>TASK 05. TRACEROUTE 도구를 사용하여 경로 테스트</b> .....	<b>12</b>

## 도전 과제

이 실습에서는 가상 네트워크의 프런트 엔드와 백 엔드 서브넷 간의 모든 트래픽이 방화벽 가상 어플라이언스를 통해 라우팅되도록 구성합니다.

- 라우팅 테이블과 라우트를 만든 다음 서브넷에 연결합니다.
- 가상 어플라이언스에서 IP 전달을 허용합니다.
- 트래픽이 가상 어플라이언스를 통해 라우팅되는지 확인합니다.

### STEP 01. 기존 가상 머신의 IP 확인

- VM2의 공용 IP 주소를 메모장에 기록합니다.
- VM3의 공용 IP 주소를 메모장에 기록합니다.

### STEP 02. 프런트 엔드 경로 테이블 구성

- RG1로<xxxxxxx> 리소스 그룹에 "app-frontend-rt" 이름의 경로 테이블을 만들고 "게이트웨이 경로 전파" 옵션은 비활성화합니다.
- app-frontend-rt 경로 테이블에 다음 속성을 사용하여 경로를 추가합니다.

속성	값
경로 이름	to-backend
대상 유형	IP 주소
대상 IP 주소/CIDR 범위	10.1.1.0/24
다음 홉 형식	가상 어플라이언스
다음 홉 주소	10.1.255.4

- app-frontend-rt 경로 테이블을 app-vnet 가상 네트워크의 frontend 서브넷에 연결합니다.

### STEP 03. 백 엔드 경로 테이블 구성

- "app-backend-rt" 이름의 경로 테이블을 만들고 게이트웨이 경로 전파는 사용하지 않도록 구성합니다.
- "app-backend-rt" 경로 테이블에 다음 속성을 사용하여 경로를 추가합니다.

속성	값
경로 이름	to-frontend
대상 유형	IP 주소
대상 IP 주소/CIDR 범위	10.1.0.0/24
다음 홉 형식	가상 어플라이언스
다음 홉 주소	10.1.255.4

- "app-backend-rt" 경로 테이블을 app-vnet 가상 네트워크의 backend 서브넷에 연결합니다.

### STEP 04. 가상 어플라이언스에 IP 전달 구성

- 다음 속성을 사용하여 [Cloud Shell]의 Bash 세션을 설정합니다.
- [Cloud Shell]의 Bash 세션에서 VM3 가상 머신에 SSH로 연결합니다.
- SSH 세션에서 `sudo sysctl` 명령을 사용하여 IP 전달을 활성화합니다.

**STEP 05. traceroute 도구를 사용하여 경로 테스트**

1. VM2 가상 머신에 SSH 세션을 연결한 후 Linux 가상 머신을 업데이트합니다.
2. VM2 가상 머신에서 traceroute 도구를 설치합니다.
3. VM2 가상 머신에서 VM1 가상 머신으로 트래픽을 전송한 후 해당 트래픽이 가상 어플라이언스(VM3)를 통해 VM1 가상 머신으로 전달되는지 확인합니다.

## TASK 01. 기존 가상 머신의 IP 확인

1. Azure 포털의 검색창에서 "가상 머신"을 검색한 후 클릭합니다. [가상 머신] 블레이드에서 VM2 가상 머신을 클릭합니다.

가상 머신 [cloudslice\(cloudslice.onmicrosoft.com\)](#)

+ 만들기 > > 클래식으로 전환 > 예약 > 보기 관리 > 새로 고침 > CSV로 내보내기 > 쿼리 열기 > 태그 지정 > 시작 ...

필드 필터링... 구독 같음 모두 형식 같음 모두 리소스 그룹 같음 모두 < 위치 같음 모두 < > 필터 추가

1 - 3/3개 레코드를 표시합니다. 그룹화 안 함 목록 보기

<input type="checkbox"/>	이름 ↑↓	형식 ↑↓	구독 ↑↓	리소스 그룹 ↑↓	위치 ↑↓	상태 ↑↓	운영 체제 ↑↓
<input type="checkbox"/>	VM1	가상 머신	Challenge Labs 7	RG1lod33435134	East US	실행 중	Linux
<input checked="" type="checkbox"/>	VM2	가상 머신	Challenge Labs 7	RG1lod33435134	East US	실행 중	Linux
<input type="checkbox"/>	VM3	가상 머신	Challenge Labs 7	RG1lod33435134	East US	실행 중	Linux

2. [VM2 가상 머신] 블레이드의 [개요]에서 공용 IP 주소를 확인한 후 메모장에 기록합니다.

VM2 가상 머신

검색 < > 연결 > 시작 < 다시 시작 < 중지 < 캡처 < 삭제 < 새로 고침 < 모바일에서 열기 < 피드백 ...

개요 활동 로그 액세스 제어(IAM) 태그 문제 진단 및 해결 설정 네트워킹 연결

기본 정보

리소스 그룹 (이동) [RG1lod33435134](#)

상태 실행 중

위치 East US

구독 (이동) [Challenge Labs 7](#)

구독 ID 8d7ebc7f-6c63-47b5-bbdc-6df02452b2bd

운영 체제 Linux (ubuntu 18.04)

VM 가용성 상태 -

크기 Standard DS1 v2(1개 vcpu, 3.5GiB 메모리)

공용 IP 주소 [20.163.184.42](#)

가상 네트워크/서브넷 [app-vnet/backend](#)

JSON 보기

3. 동일한 방법으로 [VM3 가상 머신] 블레이드의 [개요]에서 공용 IP 주소를 확인한 후 메모장에 기록합니다.

VM3 가상 머신

검색 < > 연결 > 시작 < 다시 시작 < 중지 < 캡처 < 삭제 < 새로 고침 < 모바일에서 열기 < 피드백 ...

개요 활동 로그 액세스 제어(IAM) 태그 문제 진단 및 해결 설정 네트워킹 연결

기본 정보

리소스 그룹 (이동) [RG1lod33435134](#)

상태 실행 중

위치 East US

구독 (이동) [Challenge Labs 7](#)

구독 ID 8d7ebc7f-6c63-47b5-bbdc-6df02452b2bd

운영 체제 Linux (ubuntu 18.04)

VM 가용성 상태 -

크기 Standard DS1 v2(1개 vcpu, 3.5GiB 메모리)

공용 IP 주소 [20.172.149.184](#)

가상 네트워크/서브넷 [app-vnet/dmz](#)

JSON 보기

## TASK 02. 프런트 엔드 경로 테이블 구성

1. Azure 포털의 검색창에서 "경로 테이블"을 검색한 후 클릭합니다. [경로 테이블] 블레이드의 메뉴에서 [만들기]를 클릭합니다.





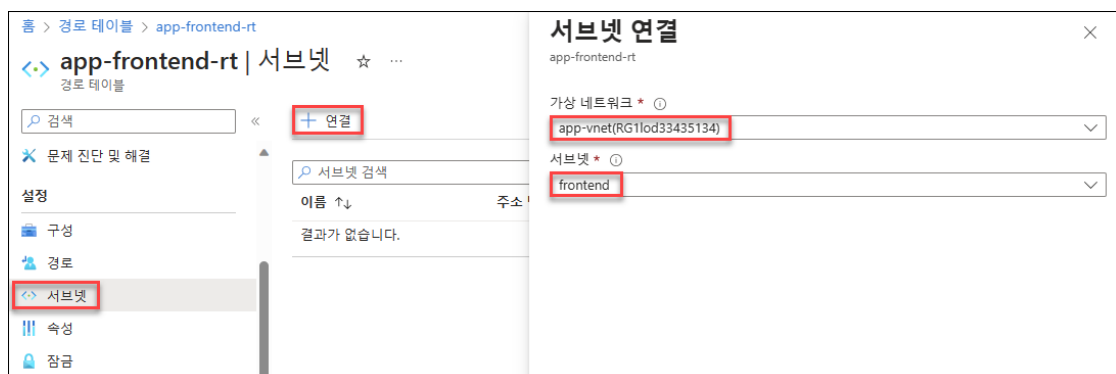
2. [Route table 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

- [프로젝트 정보 - 리소스 그룹]: RG1lod<xxxxxxxx>
- [인스턴스 정보 - 지역]: East US
- [인스턴스 정보 - 이름]: app-frontend-rt
- [인스턴스 정보 - 게이트웨이 경로 전파]: No

3. 이 작업은 `New-AzRouteTable` PowerShell 명령어나 `az network route-table` Azure CLI 명령으로 진행할 수 있습니다.
4. 새로 만든 [app-frontend-rt] 경로 테이블 블레이드로 이동합니다. [설정 - 경로]로 이동한 후 메뉴에서 [추가]를 클릭합니다. [경로 추가] 창에서 아래와 같이 구성한 후 [추가]를 클릭합니다.
  - 경로 이름: to-backend
  - 대상 유형: IP 주소
  - 대상 IP 주소/CIDR 범위: 10.1.1.0/24
  - 다음 홉 형식: 가상 어플라이언스
  - 다음 홉 주소: 10.1.255.4



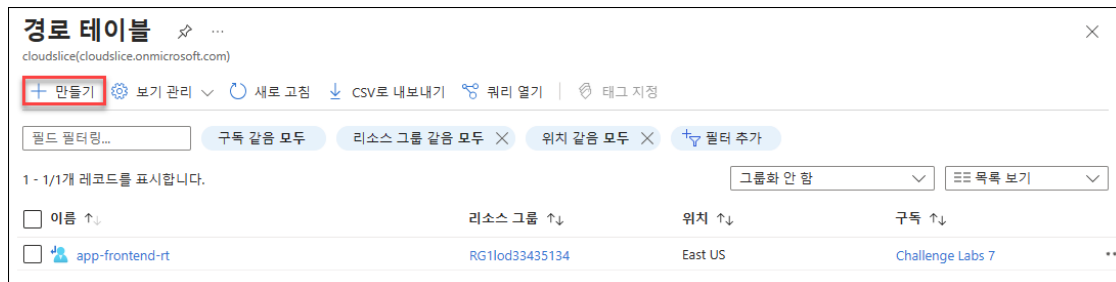
5. 이 작업은 `Get-AzRouteTable`, `Add-AzRouteConfig`, `Set-AzRouteTable` PowerShell 명령이나 `az network route-table route` Azure CLI 명령을 사용하여 구성할 수도 있습니다.
6. [app-frontent-rt 경로 테이블] 블레이드의 [설정 - 서브넷]으로 이동한 후 메뉴에서 [연결]을 클릭합니다. [서브넷 연결] 창에서 아래와 같이 구성한 후 [확인]을 클릭합니다.
  - 가상 네트워크: app-vnet(RG1lod<xxxxxxxx>)
  - 서브넷: frontend



7. 동일한 작업을 `Set-AzVirtualNetworkSubnetConfig`, `Set-AzVirtualNetwork` PowerShell 명령이나 `az network route-table route` Azure CLI 명령으로 구성할 수도 있습니다.

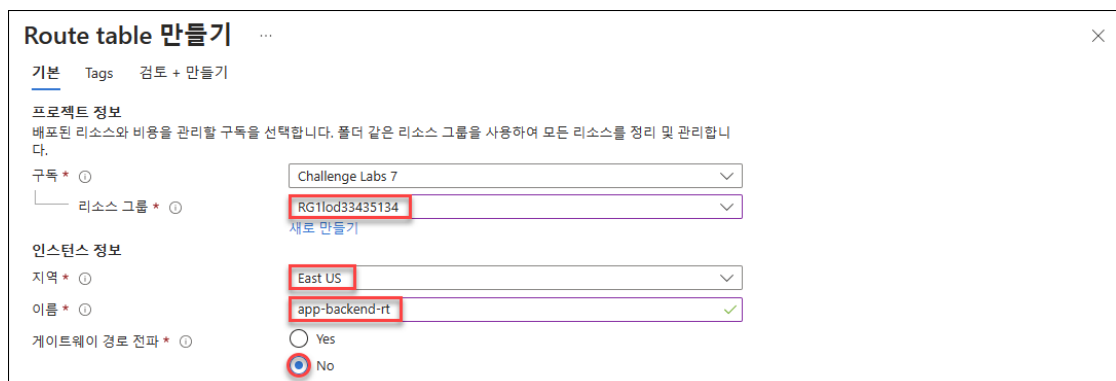
### TASK 03. 백 엔드 경로 테이블 구성

1. Azure 포털의 검색창에서 "경로 테이블"을 검색한 후 클릭합니다. [경로 테이블] 블레이드의 메뉴에서 [만들기]를 클릭합니다.



2. [Route table 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

- [프로젝트 정보 - 리소스 그룹]: RG1lod<xxxxxxxx>
- [인스턴스 정보 - 지역]: East US
- [인스턴스 정보 - 이름]: app-backend-rt
- [인스턴스 정보 - 게이트웨이 경로 전파]: No



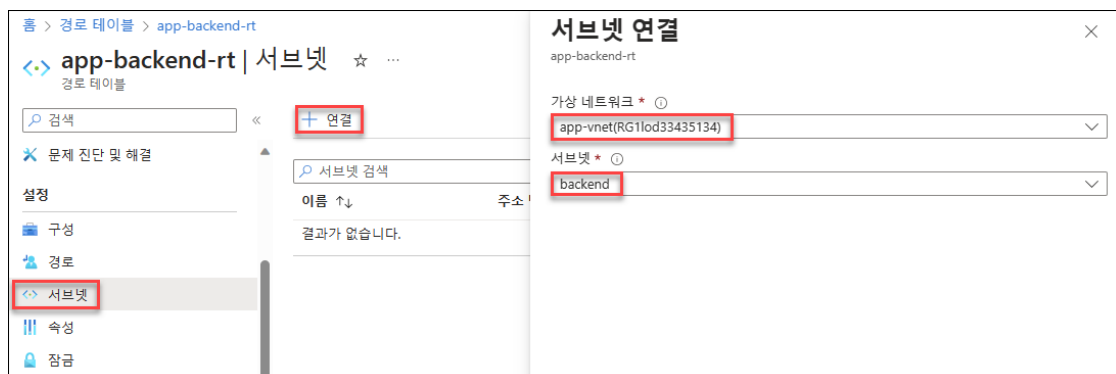
3. 새로 만든 [app-backend-rt] 경로 테이블 블레이드의 [설정 - 경로]로 이동한 후 [추가]를 클릭합니다. [경로 추가] 창에서 아래와 같이 구성한 후 [추가]를 클릭합니다.

- 경로 이름: to-frontend
- 대상 유형: IP 주소
- 대상 IP 주소/CIDR 범위: 10.1.0.0/24
- 다음 홉 형식: 가상 어플라이언스
- 다음 홉 주소: 10.1.255.4



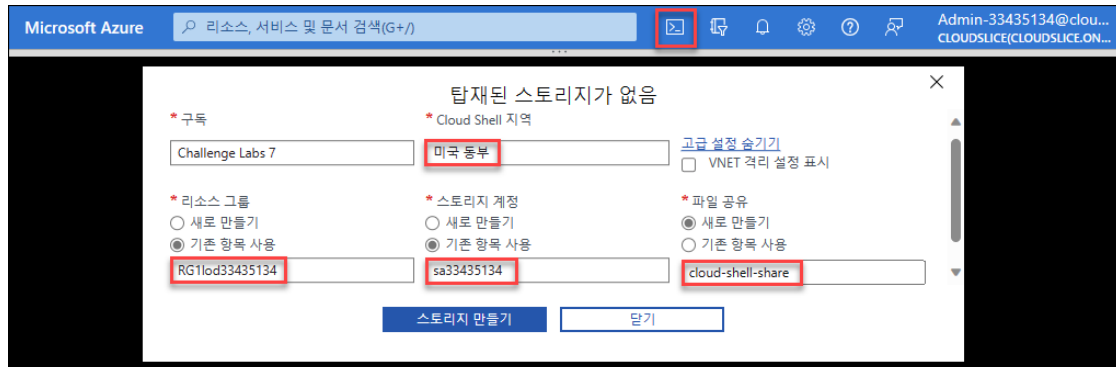
4. [app-backend-rt 경로 테이블] 블레이드의 [설정 - 서브넷]으로 이동한 후 메뉴에서 [연결]을 클릭합니다. [서브넷 연결] 창에서 아래와 같이 구성한 후 [확인]을 클릭합니다.

- 가상 네트워크: app-vnet(RG1lod<xxxxxxxx>)
- 서브넷: backend



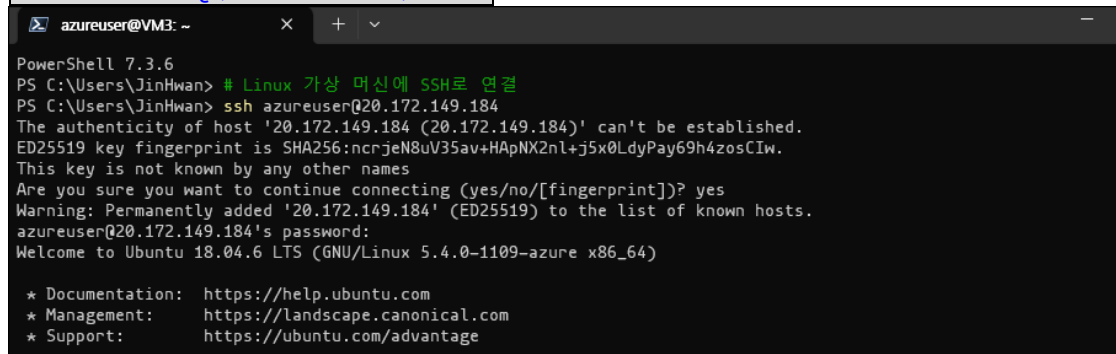
#### TASK 04. 가상 어플라이언스에 IP 전달 구성

- Azure 포털에서 [Cloud Shell]을 클릭한 후 "Bash"를 클릭합니다. [탑재된 스토리지가 없음] 창에서 "고급 설정 표시" 링크를 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<xxxxxxxx>" 리소스 그룹을 선택합니다.
  - 스토리지 계정: "기존 항목 사용"을 선택한 후 "sa<xxxxxxxx>" 스토리지 계정을 선택합니다.
  - 파일 공유: "새로 만들기"를 선택한 후 "cloud-shell-share" 이름을 입력합니다.



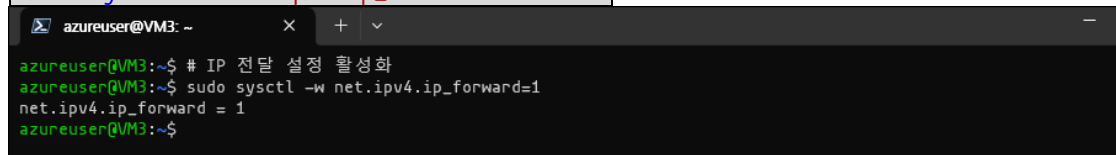
- 실습 환경에서 [Cloud Shell]의 Bash 세션에서 SSH 연결이 권한 문제로 실행되지 않는 경우가 많습니다. 이 경우 자신이 컴퓨터에 있는 [터미널]을 사용합니다.
- [터미널]에서 다음 명령을 실행하여 VM3 가상 머신에 SSH 연결을 설정합니다. 암호는 "AzurePwd<xxxxxxxx>"입니다.

```
# Linux 가상 머신에 SSH로 연결
ssh azureuser@<VM3 Public IP>
```



- [터미널]에서 다음 명령을 실행하여 IP 전달을 활성화합니다.

```
# IP 전달 설정 활성화
sudo sysctl -w net.ipv4.ip_forward=1
```



## TASK 05. traceroute 도구를 사용하여 경로 테스트

- 자신의 컴퓨터에서 [터미널]을 실행한 후 다음 명령을 실행하여 VM2 가상 머신에 SSH로 연결합니다.

```
# VM2 가상 머신에 SSH 연결
ssh azureuser@<VM2 Public IP>
```

```

azureuser@VM2: ~
PS C:\Users\JinHwan> # VM2 가상 머신에 SSH 연결
PS C:\Users\JinHwan> ssh azureuser@20.163.184.42
The authenticity of host '20.163.184.42 (20.163.184.42)' can't be established.
ED25519 key fingerprint is SHA256:JLmMk0G8MC/VQedqzJknhgRcz0thjTJ2aeUI060r5+8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.163.184.42' (ED25519) to the list of known hosts.
azureuser@20.163.184.42's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1109-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

```

2. [터미널]에서 다음 명령을 실행하여 Linux 가상 머신을 업데이트합니다.

```
# Linux 가상 머신 업데이트
sudo apt-get update
```

```

azureuser@VM2: ~$ # Linux 가상 머신 업데이트
azureuser@VM2:~$ sudo apt-get update
Hit:1 http://azure.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu bionic-backports InRelease [83.3 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:5 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [8570 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu bionic/universe Translation-en [4941 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [151 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse Translation-en [108 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [3045 kB]
Get:10 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [553 kB]

```

3. [터미널]에서 다음 명령을 실행하여 traceroute 도구를 설치합니다.

```
# traceroute 도구 설치
sudo apt install traceroute
```

```

azureuser@VM2: ~$ # traceroute 도구 설치
azureuser@VM2:~$ sudo apt install traceroute
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
traceroute
0 upgraded, 1 newly installed, 0 to remove and 7 not upgraded.
Need to get 45.4 kB of archives.
After this operation, 152 kB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 traceroute amd64 1:2.1.0-2 [45.4 kB]

```

4. [터미널]에서 다음 명령을 실행하여 VM2 가상 머신에서 VM1 가상 머신에 대한 경로를 확인합니다. 트래픽이 VM3 (가상 어플라이언스)를 통해 처리되는 것을 확인합니다.

```
# VM1 가상 머신에 대한 경로 확인
traceroute VM1
```

```

azureuser@VM2: ~$ # VM1 가상 머신에 대한 경로 확인
azureuser@VM2:~$ traceroute VM1
traceroute to VM1 (10.1.0.4), 30 hops max, 60 byte packets
 1 vm3.internal.cloudapp.net (10.1.255.4) 1.997 ms 3.047 ms 3.020 ms
 2 vm1.internal.cloudapp.net (10.1.0.4) 4.092 ms * *
azureuser@VM2:~$

```