한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. LAB06

트래픽 관리 구현

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

Microsoft Technical Trainer

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.

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 허여되지 아니합니다.

© 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
2021.11.20	1.0.0	우진환	LAB06 작성
2022.10.07	1.1.0	우진환	Azure 포털 변경 사항 적용
2023.02.08	1.2.0	우진환	Cloudslice 변경 사항 적용
2023.06.02	1.3.0	우진환	Cloudslice 변경 사항 적용
2023.08.31	1.3.5	우진환	피어링, 부하 분산 장치, 애플리케이션 게이트웨이 UI 업데이트

Microsoft

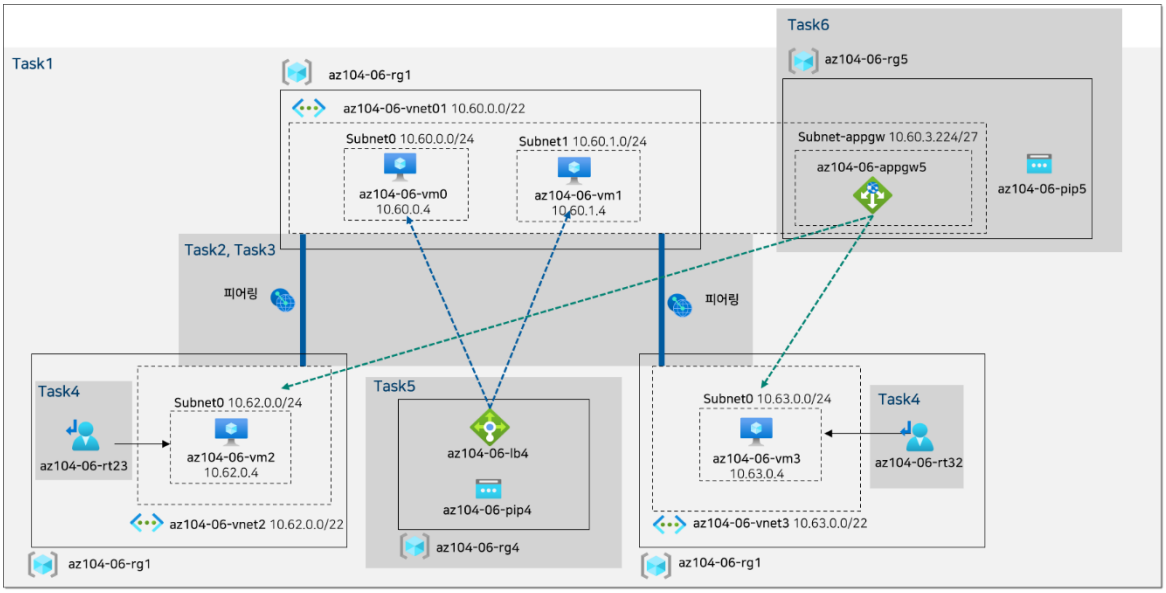
목차

Microsoft

실습 시나리오

여러분은 Contoso가 Azure 환경에서 구현하려고 하는 허브 및 스포크(hub and spoke) 네트워크 토폴로지에서 Azure 가상 머신을 대상으로 하는 네트워크 트래픽 관리를 테스트해야 합니다. 이전 실습에서는 메시(mesh) 토폴로지를 구성했습니다. 이 테스트에는 허브를 통해 트래픽을 강제로 흐르게 하는 사용자 정의 경로(user defined route)를 사용하여 스포크 간 연결을 구현합니다. 또한 4 계층 및 7 계층의 로드 밸런서를 사용하여 가상 머신에 대한 트래픽을 분산하는 것도 포함되어야 합니다. 이를 위해 Azure Load Balancer (4 계층)와 Azure Application Gateway (7 계층)를 사용하려고 합니다.

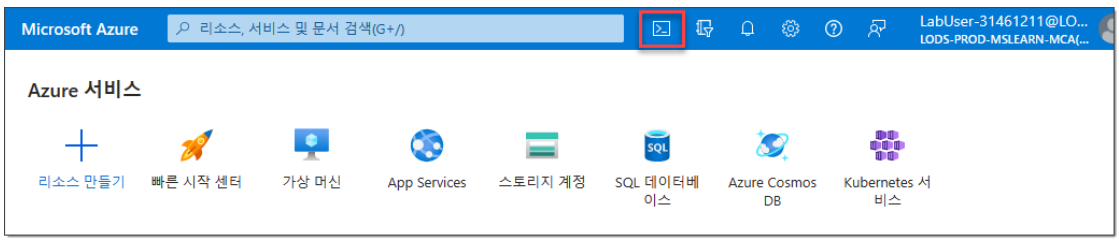
아키텍처 다이어그램



TASK 01. 실습 환경 프로비전

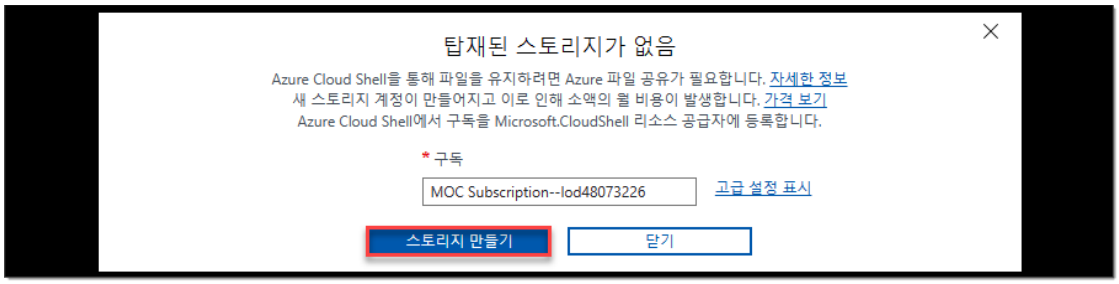
이 작업에서는 동일한 Azure 지역에 4대의 가상 머신을 배포합니다. 첫 번째 2대의 가상 머신은 허브 가상 네트워크에 배포되고 나머지 2대의 가상 머신은 별도의 스포크 가상 네트워크에 배포됩니다.

1. Azure 포털의 우측 상단에서 [Cloud Shell]을 클릭합니다.

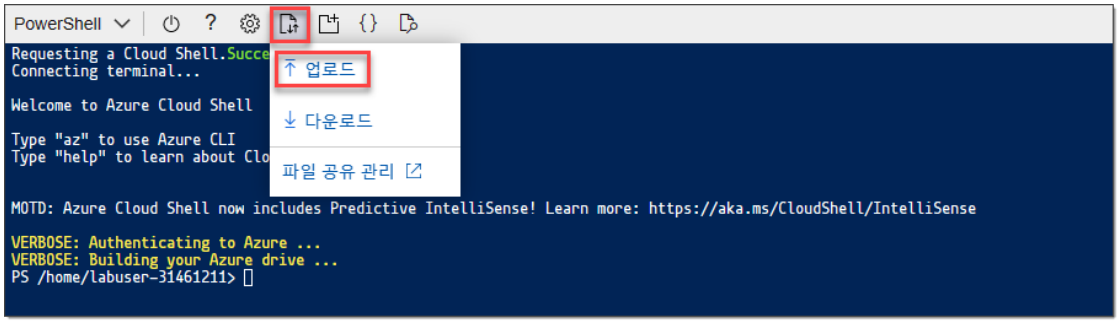


2. [Azure Cloud Shell 시작] 창에서 [PowerShell]을 클릭합니다.

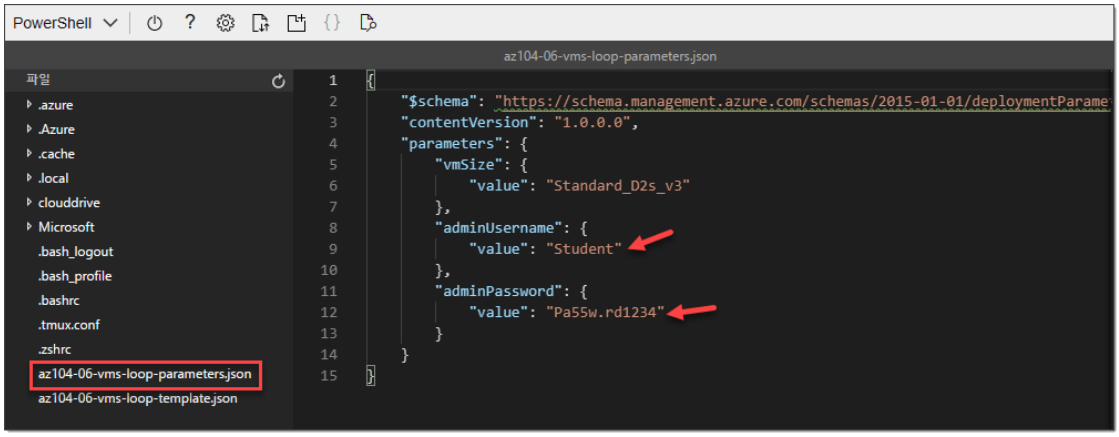
3. [탑재된 스토리지가 없음] 페이지에서 [스토리지 만들기]를 클릭합니다.



4. Azure 포털에서 [Cloud Shell]을 실행합니다. [Cloud Shell]의 [파일 업로드/다운로드] 아이콘을 클릭한 후 [업로드]를 클릭합니다. "`Labs\06\az104-06-vms-loop-template.json`" 파일과 "`Labs\06\az104-06-vms-loop-parameters.json`" 파일을 업로드합니다.



5. 실습에서 가상 머신 로그온에 사용되는 사용자 계정과 암호를 변경하고자 하는 경우 [Cloud Shell]에서 [편집기 열기]를 클릭한 후 `az104-06-vms-loop-parameters.json` 파일을 열고 계정과 암호를 변경할 수 있습니다.



6. [Cloud Shell]에서 다음 명령을 실행하여 실습 환경을 호스팅할 리소스 그룹을 만듭니다.

```
# 실습에서 사용할 리소스 그룹 만들기
$location = 'eastus'
```

```
$rgName = 'az104-06-rg1'

New-AzResourceGroup -Name $rgName -Location $location
```

```
PS /home/labuser-31461211> # 실습에서 사용할 리소스 그룹 만들기
PS /home/labuser-31461211> $location = 'eastus'
PS /home/labuser-31461211> $rgName = 'az104-06-rg1'
PS /home/labuser-31461211>
PS /home/labuser-31461211> New-AzResourceGroup -Name $rgName -Location $location

ResourceGroupName : az104-06-rg1
Location          : eastus
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/e50ede69-8a2b-4afc-8473-7972f2b6d297/resourceGroups/az104-06-rg1


PS /home/labuser-31461211>
```

7. [Cloud Shell]에서 다음 명령을 실행하여 업로드한 템플릿 파일과 매개 변수 파일을 사용하여 3개의 가상 네트워크를 만들고 4대의 Azure VM을 만듭니다. 배포에 5분 정도 시간이 소요됩니다.

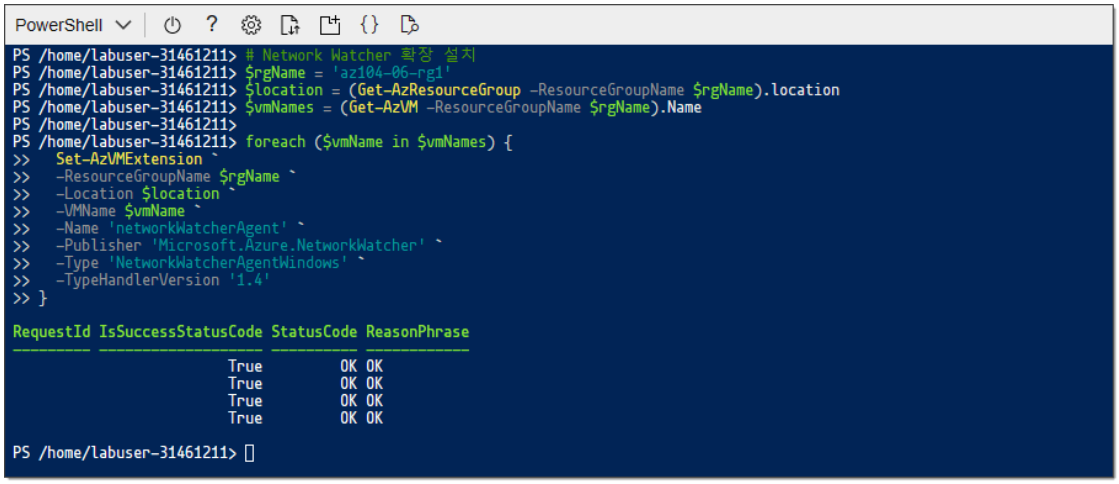
```
# 실습에 사용할 리소스 배포
New-AzResourceGroupDeployment `
  -ResourceGroupName $rgName `
  -TemplateFile $HOME/az104-06-vms-loop-template.json `
  -TemplateParameterFile $HOME/az104-06-vms-loop-parameters.json
```

```
PS /home/labuser-31461211> # 실습에 사용할 리소스 배포
PS /home/labuser-31461211> New-AzResourceGroupDeployment `
>>   -ResourceGroupName $rgName `
>>   -TemplateFile $HOME/az104-06-vms-loop-template.json `
>>   -TemplateParameterFile $HOME/az104-06-vms-loop-parameters.json

DeploymentName          : az104-06-vms-loop-template
ResourceGroupName       : az104-06-rg1
ProvisioningState       : Succeeded
Timestamp               : 6/1/2023 6:43:04 AM
Mode                    : Incremental
TemplateLink            :
Parameters              :
                          Name             Type                       Value
                          ===============  =========================  ==========
                          vmSize           String                     "Standard_D2s_v3"
                          vmName           String                     "az104-06-vm"
                          vmCount          Int                        4
                          adminUsername    String                     "Student"
                          adminPassword    SecureString               null

Outputs                 :
DeploymentDebugLogLevel :
```

8. [Cloud Shell]에서 다음 명령을 실행하여 배포한 Azure VM에 Network Watcher 확장을 설치합니다. 확장 배포에 5분 정도가 소요됩니다.

```
# Network Watcher 확장 설치
$rgName = 'az104-06-rg1'
$location = (Get-AzResourceGroup -ResourceGroupName $rgName).location
$vmNames = (Get-AzVM -ResourceGroupName $rgName).Name

foreach ($vmName in $vmNames) {
  Set-AzVMExtension `
  -ResourceGroupName $rgName `
  -Location $location `
  -VMName $vmName `
  -Name 'networkWatcherAgent' `
  -Publisher 'Microsoft.Azure.NetworkWatcher' `
  -Type 'NetworkWatcherAgentWindows' `
  -TypeHandlerVersion '1.4'
}
```


Microsoft



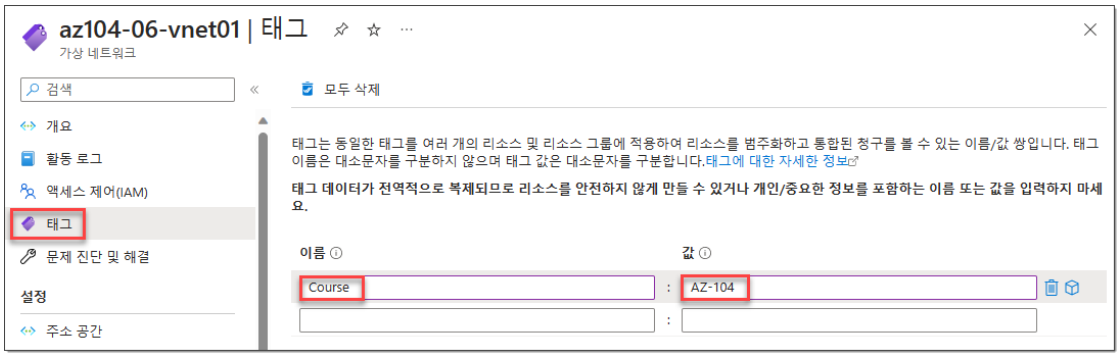
9. [Cloud Shell]을 닫습니다.

TASK 02. 허브 및 스포크 네트워크 토폴로지 구성

이 작업에서는 허브 및 스포크 네트워크 토폴로지를 만들기 위해 이전에 배포한 가상 네트워크 간에 로컬 피어링을 구성합니다.

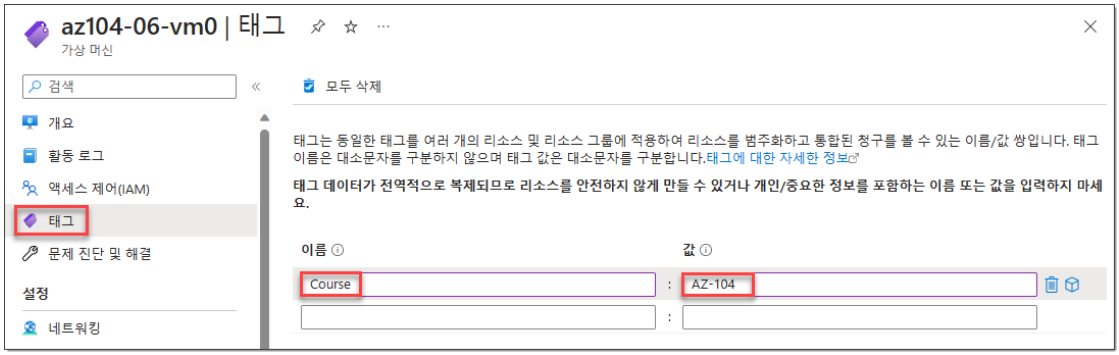
1. Azure 포털에서 [`az104-06-rg1` 리소스 그룹] 블레이드로 이동한 후 `az104-06-vnet01` 가상 네트워크 리소스를 클릭합니다.

2. [`az104-06-vnet01` 가상 네트워크] 블레이드의 [태그]로 이동합니다. 태그 이름(`Course`)과 값(`AZ-104`)을 입력한 후 [적용]을 클릭합니다.



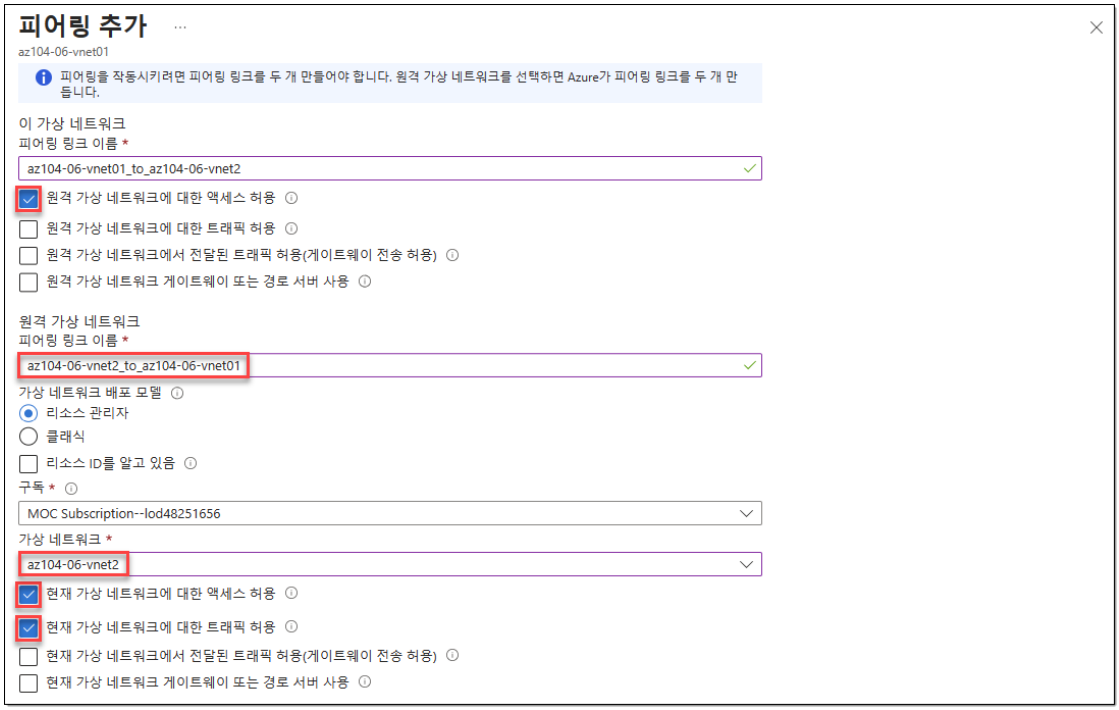
3. 위 작업은 반복하여 `az-104-06-vnet2`, `az104-06-vnet3` 가상 네트워크에도 동일한 태그와 값을 설정합니다.
4. [`az104-06-rg1` 리소스 그룹] 블레이드에서 `az104-06-vm0` 가상 머신 리소스를 클릭합니다.

5. [`az104-06-vm0` 가상 머신] 리소스의 [태그]로 이동합니다. 태그 이름(`Course`)과 값(`AZ-104`)을 입력한 후 [적용]을 클릭합니다.

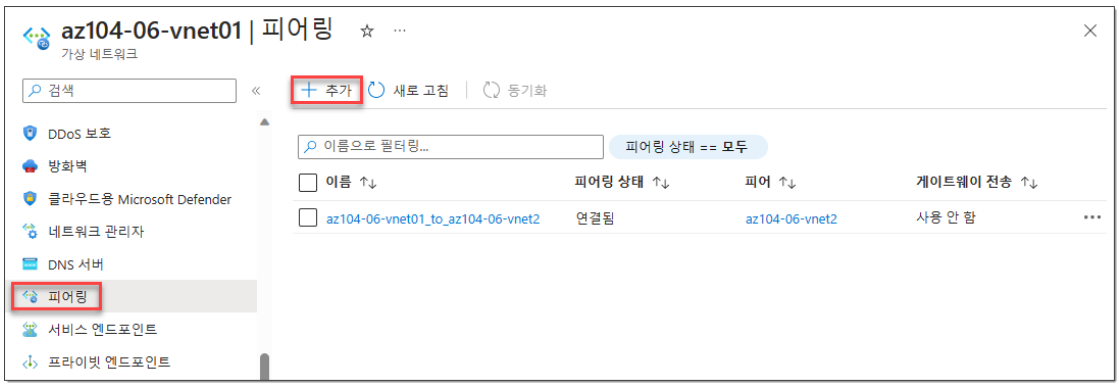


6. 이 작업을 반복하여 `az104-06-vm1`, `az104-06-vm2`, `az104-06-vm3` 가상 머신에도 동일한 태그 이름과 값을 지정합니다. 이 작업은 프로덕션 환경에서 수행할 필요는 없으며 실습 환경에서 Azure의 리소스가 더 빨리 포털 UI에서 표시하기 위한 작업입니다. 또는 Azure 포털에서 가상 네트워크 피어링을 만들 때 간혹 새로 프로비저닝한 가상 네트워크가 표시되지 않는 문제를 해결하기 위해 "`리소스 ID`"를 직접 사용할 수 있습니다. 혹은 각 가상 네트워크에 임의의 태그를 추가하여 Azure 포털 변경 사항을 즉시 적용할 수도 있습니다.
7. [`az104-06-vnet01` 가상 네트워크] 블레이드로 이동합니다. [`az104-06-vnet01` 가상 네트워크] 블레이드의 [설정 - 피어링]으로 이동한 후 [추가]를 클릭합니다.

8. [피어링 추가]에서 다음과 같이 구성한 후 [추가]를 클릭합니다.
   - [이 가상 네트워크 - 피어링 링크 이름]: az104-06-vnet01_to_az104-06-vnet2
   - [이 가상 네트워크 - 원격 가상 네트워크에 대한 액세스 허용]: 선택합니다.
   - [이 가상 네트워크 - 원격 가상 네트워크에 대한 트래픽 허용]: 선택하지 않습니다.
   - [이 가상 네트워크 - 원격 가상 네트워크에서 전달된 트래픽 허용(게이트웨이 전송 허용)]: 선택하지 않습니다.
   - [이 가상 네트워크 - 원격 가상 네트워크 게이트웨이 또는 경로 서버 사용]: 선택하지 않습니다.
   - [원격 가상 네트워크 - 피어링 링크 이름]: az104-06-vnet2_to_az104-06-vnet01
   - [원격 가상 네트워크 - 가상 네트워크 배포 모델]: 리소스 관리자
   - [원격 가상 네트워크 - 리소스 ID를 알고 있음]: 선택하지 않음
   - [원격 가상 네트워크 - 가상 네트워크]: az104-06-vnet2
   - [원격 가상 네트워크 - 현재 가상 네트워크에 대한 액세스 허용]: 선택합니다.
   - [원격 가상 네트워크 - 현재 가상 네트워크에 대한 트래픽 허용]: 선택하지 않습니다.
   - [원격 가상 네트워크 - 현재 가상 네트워크에서 전달된 트래픽 허용(게이트웨이 전송 허용]: 선택하지 않습니다.
   - [원격 가상 네트워크 - 현재 가상 네트워크 게이트웨이 또는 경로 서버 사용]: 선택하지 않습니다.

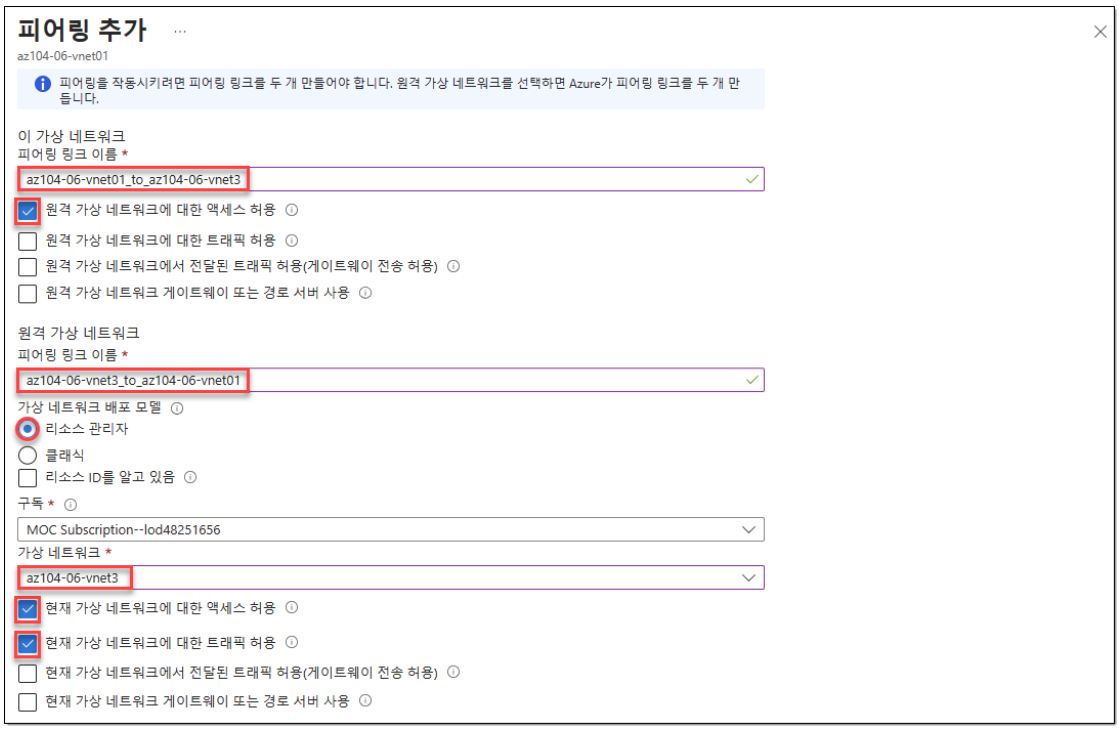


9. 작업이 완료될 때까지 기다립니다. 이 단계에서 `az104-06-vnet1`과 `az104-06-vnet2` 가상 네트워크 간 두 개의 로컬 피어링이 구성됩니다.
10. [`az104-06-vnet01` 가상 네트워크] 블레이드의 [설정 - 피어링]에서 다시 [추가]를 클릭합니다.



11. [피어링 추가]에서 다음과 같이 구성한 후 [추가]를 클릭합니다.
    - [이 가상 네트워크 - 피어링 링크 이름]: az104-06-vnet01_to_az104-06-vnet3
    - [이 가상 네트워크 - 원격 가상 네트워크에 대한 액세스 허용]: 선택합니다.
    - [이 가상 네트워크 - 원격 가상 네트워크에 대한 트래픽 허용]: 선택하지 않습니다.
    - [이 가상 네트워크 - 원격 가상 네트워크에서 전달된 트래픽 허용(게이트웨이 전송 허용)]: 선택하지 않습니다.
    - [이 가상 네트워크 - 원격 가상 네트워크 게이트웨이 또는 경로 서버 사용]: 선택하지 않습니다.
    - [원격 가상 네트워크 - 피어링 링크 이름]: az104-06-vnet3_to_az104-06-vnet01
    - [원격 가상 네트워크 - 가상 네트워크 배포 모델]: 리소스 관리자
    - [원격 가상 네트워크 - 리소스 ID를 알고 있음]: 선택하지 않음
    - [원격 가상 네트워크 - 가상 네트워크]: az104-06-vnet2

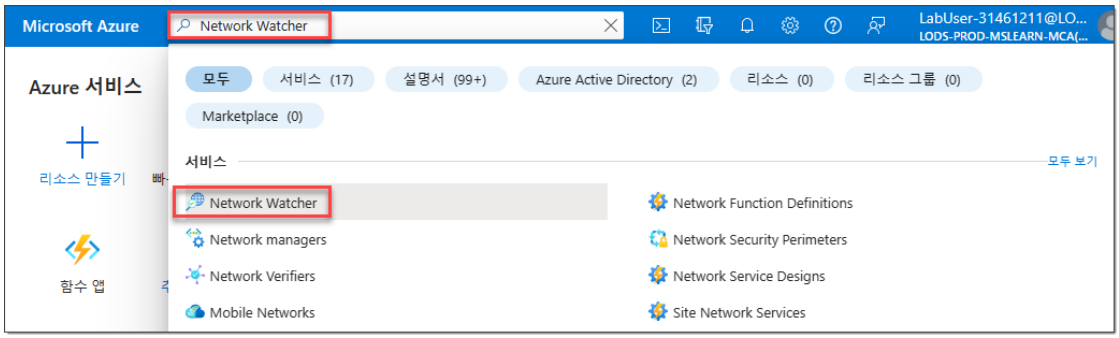
- [원격 가상 네트워크 - 현재 가상 네트워크에 대한 액세스 허용]: 선택합니다.
- [원격 가상 네트워크 - 현재 가상 네트워크에 대한 트래픽 허용]: 선택하지 않습니다.
  - [원격 가상 네트워크 - 현재 가상 네트워크에서 전달된 트래픽 허용(게이트웨이 전송 허용]: 선택하지 않습니다.
  - [원격 가상 네트워크 - 현재 가상 네트워크 게이트웨이 또는 경로 서버 사용]: 선택하지 않습니다.



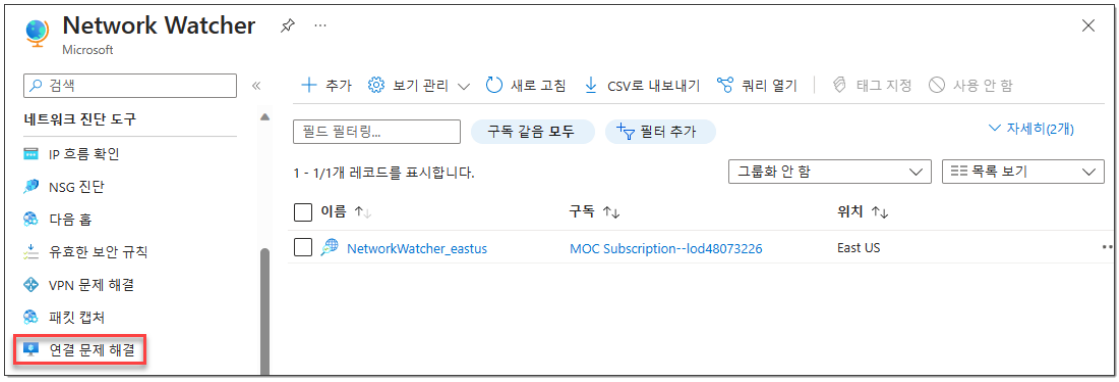
TASK 03. 가상 네트워크 피어링의 전이성(transitivity) 테스트

이 작업에서는 Network Watcher를 사용하여 가상 네트워크 피어링의 전이성을 테스트합니다.

1. Azure 포털의 검색 창에서 "`Network Watcher`"를 검색하고 클릭합니다.



2. [Network Watcher] 블레이드에서 리소스를 배포한 지역에 대한 Network Watcher가 표시되는지 확인하고 [네트워크 진단 도구 - 연결 문제 해결]을 클릭합니다.



3. [연결 문제 해결]에서 다음과 같이 구성하고 [진단 테스트 실행]을 클릭합니다.
   - [소스 - 리소스 그룹]: az104-06-rg1
   - [소스 - 원본 유형]: 가상 머신
   - [소스 - 가상 머신]: az104-06-vm0
   - [대상 주소 - 대상 유형]: 수동으로 지정
   - [대상 주소 - URI, FQDN 또는 IP 주소]: `az104-06-vm2`의 프라이빗 IP 주소인 "`10.62.0.4`"를 입력
   - [프로브 설정 - 프로토콜]: TCP
   - [프로브 설정 - 대상 포트]: 3389
   - [연결 진단 - 진단 테스트]: 모두 선택합니다.

4. 연결 확인 결과가 반환될 때까지 기다립니다. 상태가 "`연결 가능`"으로 표시되는 것을 확인합니다. 이를 통해 네트워크 경로를 검토하고 VM 간 중간 홉이 없고 대기 시간이 최소화된 직접 연결인 것을 확인할 수 있습니다. 허브 가상 네트워크가 두 번째 스포크 가상 네트워크와 직접 피어링이 되어 있기 때문에 이는 예상되는 결과입니다.

5. 동일한 방법으로 `az104-06-vm0` 가상 머신에서 `az104-06-vm3` 가상 머신으로 연결을 테스트합니다. `az104-06-vm0` 가상 머신은 허브 네트워크에 배포되었기 때문에 `az104-06-vm2` 가상 머신과 `az104-06-vm3` 가상 머신에 모두 연결할 수 있습니다.

설정	값
리소스 그룹	az104-06-rg1
원본 유형	가상 머신
가상 머신	az104-06-vm0
대상 주소	수동으로 지정
URI, FQDN 또는 IP 주소	10.63.0.4 (az104-06-vm3 가상 머신의 프라이빗 IP 주소)
프로토콜	TCP
대상 포트	3389
진단 테스트	모두 선택

6. [연결 문제 해결]에서 아래 정보를 입력한 후 [선택]을 클릭하여 `az104-06-vm2` 가상 머신과 `az104-06-vm3` 가상 머신 간의 연결을 테스트합니다.
   - [소스 - 리소스 그룹]: az104-06-rg1
   - [소스 - 원본 유형]: 가상 머신
   - [소스 - 가상 머신]: az104-06-vm2
   - [대상 주소 - 대상 유형]: 수동으로 지정
   - [대상 주소 - URI, FQDN 또는 IP 주소]: `az104-06-vm3`의 프라이빗 IP 주소인 "`10.63.0.4`"를 입력
   - [프로브 설정 - 프로토콜]: TCP
   - [프로브 설정 - 대상 포트]: 3389
   - [연결 진단 - 진단 테스트]: 모두 선택

7. 결과에서 "연결할 수 없음"이 반환되는 것을 확인합니다. 두 개의 스포크 가상 네트워크는 서로 피어링되어 있지 않기 때문에 이는 예상되는 결과입니다. 가상 네트워크 피어링은 전이적이지 않습니다.

TASK 04. 허브 및 스포크 토폴로지에 라우팅 구성

이 작업에서는 두 개의 스포크 가상 네트워크간 라우팅을 구성하고 테스트합니다. 이를 위해 `az104-06-vm0` 가상 머신의 네트워크 인터페이스에 IP 포워딩을 활성화하고 운영 체제 내에서 라우팅을 활성화하고 스포크 가상 네트워크에 사용자 지정 경로를 구성합니다.

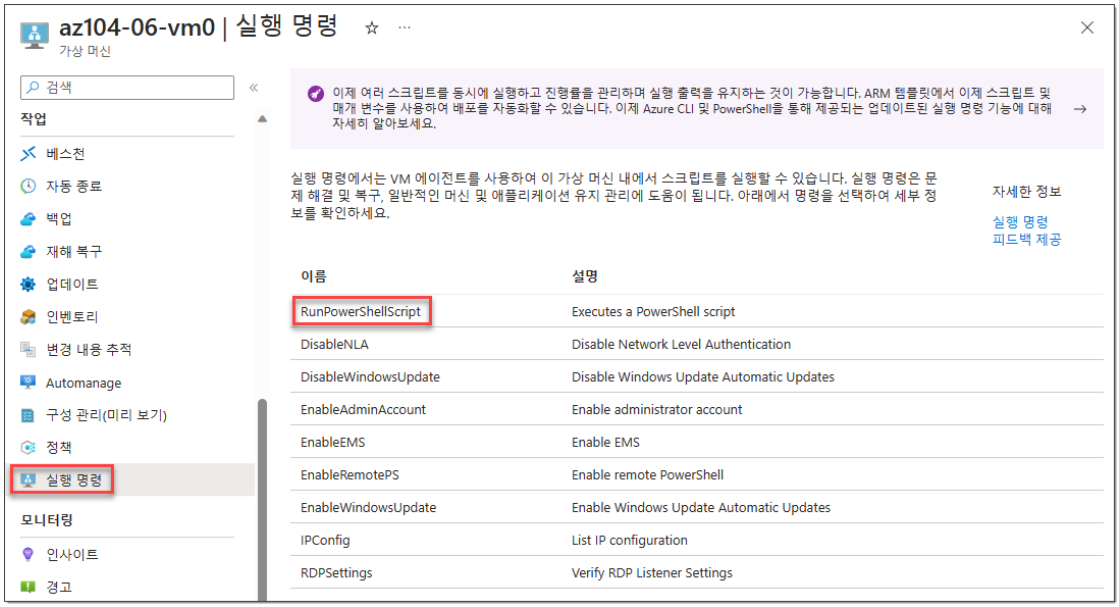
1. Azure 포털의 [`az104-06-rg1` 리소스 그룹] 블레이드로 이동한 후 `az104-06-vm0` 가상 머신을

클릭합니다.

2. [az104-06-vm0 가상 머신] 블레이드의 [설정 - 네트워킹]으로 이동한 후 네트워크 인터페이스 링크를 클릭합니다.

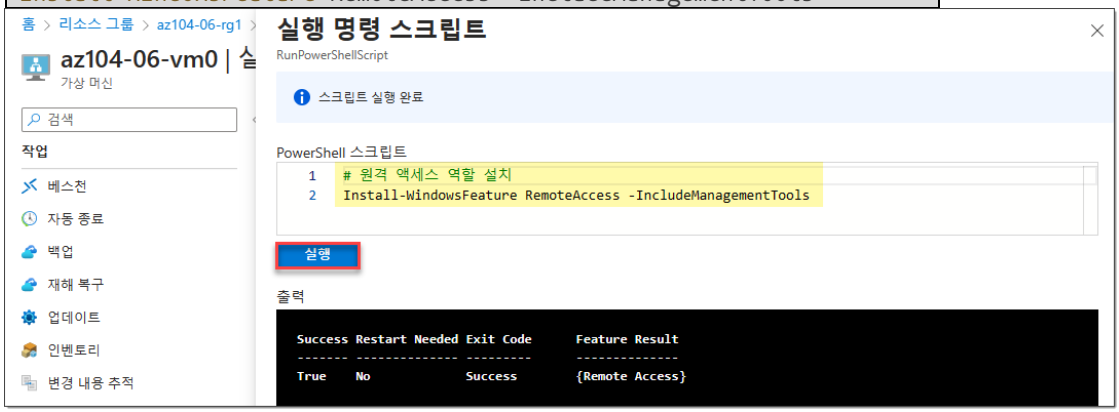
3. [az104-06-nic0 네트워크 인터페이스] 블레이드의 [설정 - IP 구성]으로 이동합니다. "IP 전달" 설정을 사용하도록 체크한 후 [적용]을 클릭합니다. 이 설정은 az104-06-vm0 가상 머신을 라우터로 구성하여 두 스포크 가상 네트워크간 트래픽을 라우팅하도록 구성하기 위해 필요합니다.

4. [az104-06-vm0 가상 머신] 블레이드의 [작업 - 실행 명령]으로 이동한 후 "RunPowerShellScript"를 클릭합니다.



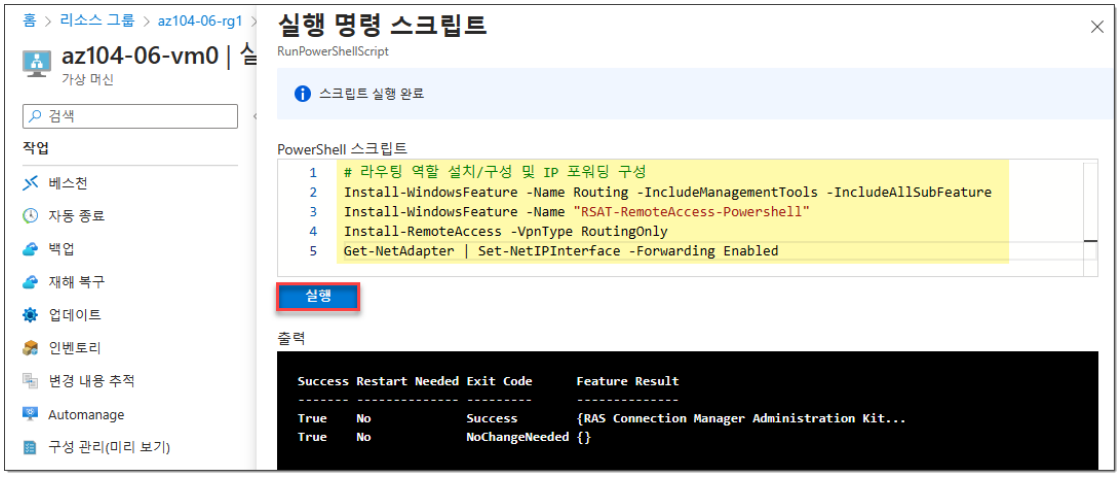
5. [실행 명령 스크립트] 창에서 다음 명령을 입력한 후 [실행]을 클릭하여 원격 액세스 Windows Server 역할을 설치합니다. 명령 실행이 완료될 때까지 기다립니다.

```
# 원격 액세스 역할 설치
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

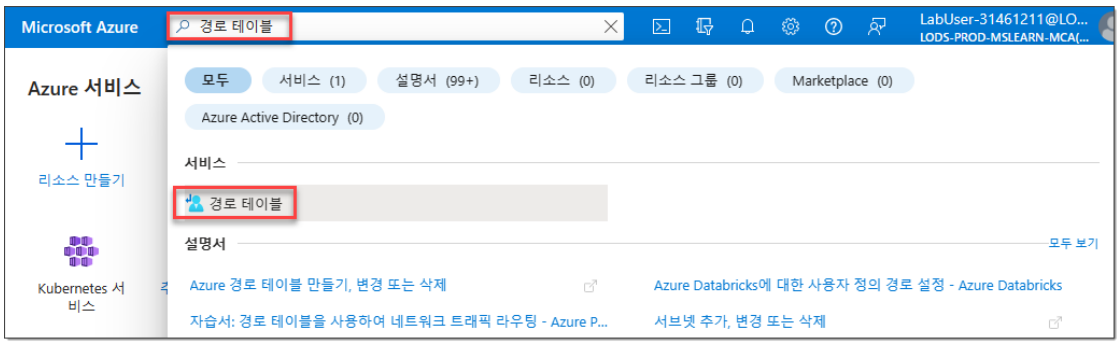


6. [실행 명령 스크립트] 창에서 다음 명령을 입력한 후 [실행]을 클릭하고 명령 실행이 완료될 때까지 기다립니다.

```
# 라우팅 역할 설치/구성 및 IP 포워딩 구성
Install-WindowsFeature -Name Routing -IncludeManagementTools `
 -IncludeAllSubFeature
Install-WindowsFeature -Name "RSAT-RemoteAccess-Powershell"
Install-RemoteAccess -VpnType RoutingOnly

Get-NetAdapter | Set-NetIPInterface -Forwarding Enabled
```

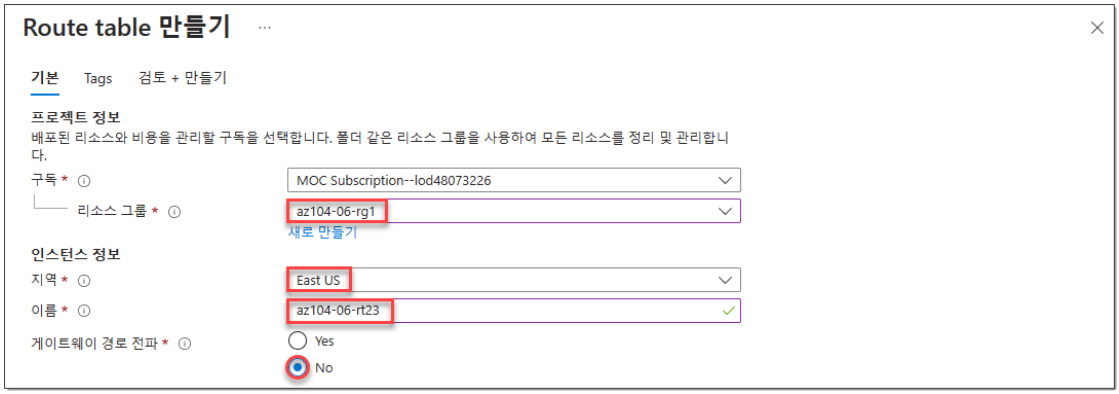


7. Azure 포털의 검색창에서 "경로 테이블"을 검색한 후 클릭합니다.



8. [경로 테이블] 블레이드의 메뉴에서 [만들기]를 클릭합니다.

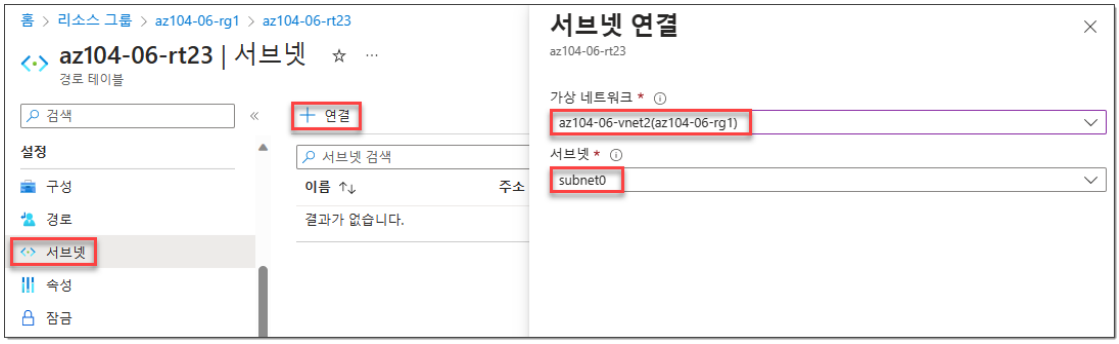
9. [Route table 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: az104-06-rg1
   - [인스턴스 정보 - 지역]: East US
   - [인스턴스 정보 - 이름]: az104-06-rt23
   - [인스턴스 정보 - 게이트웨이 경로 전파]: No



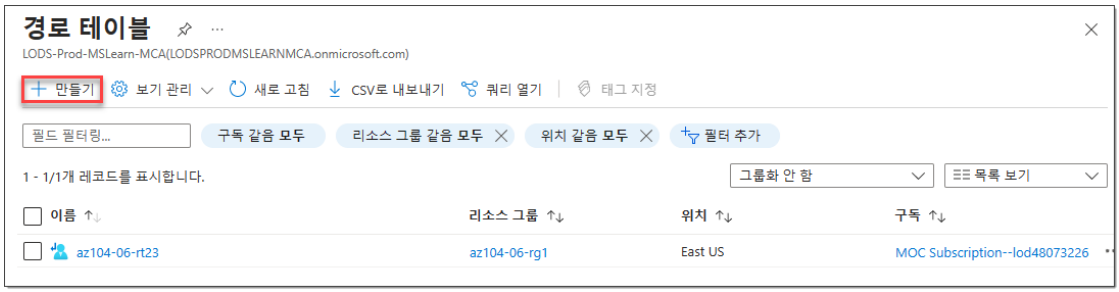
10. 배포가 완료되면 [리소스로 이동]을 클릭합니다. [`az104-06-rt23` 경로 테이블] 블레이드의 [설정 - 경로]로 이동한 후 메뉴에서 [추가]를 클릭합니다.

11. [경로 추가] 창에서 다음과 같이 구성하고 [추가]를 클릭합니다.
    - 경로 이름: az104-06-route-vnet2-to-vnet3
    - 대상 주소 접두사: IP 주소
    - 대상 IP 주소/CIDR 범위: 10.63.0.0/20
    - 다음 홉 형식: 가상 어플라이언스
    - 다음 홉 주소: 10.60.0.4

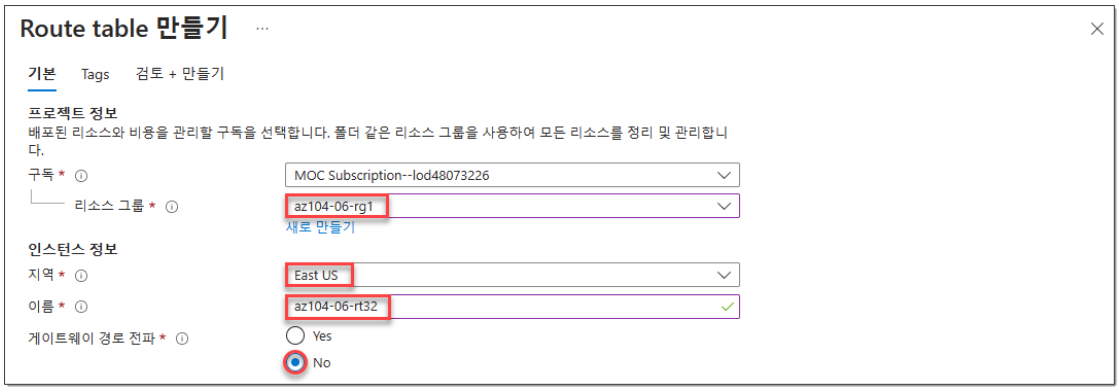
12. [`az104-06-rt23` 경로 테이블] 블레이드의 [설정 - 서브넷]으로 이동한 후 [연결]을 클릭합니다. [서브넷 연결] 창에서 다음과 같이 구성한 후 [확인]을 클릭합니다.
    - 가상 네트워크: az104-06-vnet2(az104-06-rg1)
    - 서브넷: subnet0



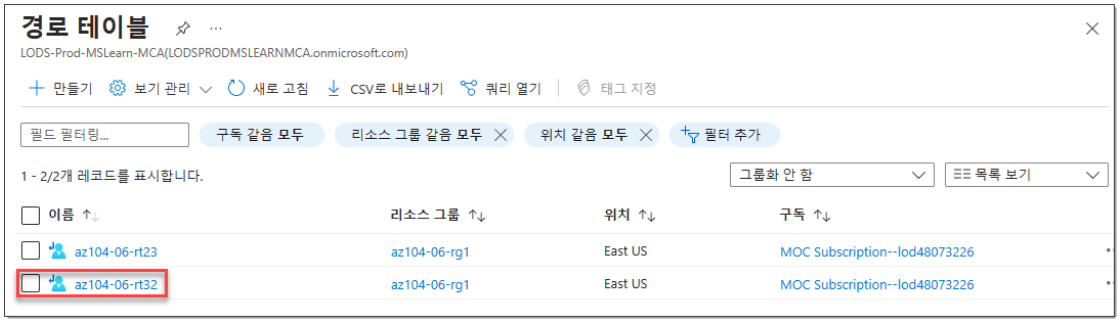
13. Azure 포털의 검색창에서 "경로 테이블"을 검색한 후 클릭합니다. [경로 테이블] 블레이드의 메뉴에서 [만들기]를 클릭합니다.



14. [Route table 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성하고 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
    - [프로젝트 정보 - 리소스 그룹]: az104-06-rg1
    - [인스턴스 정보 - 지역]: East US
    - [인스턴스 정보 - 이름]: az104-06-rt32
    - [인스턴스 정보 - 게이트웨이 경로 전파]: No

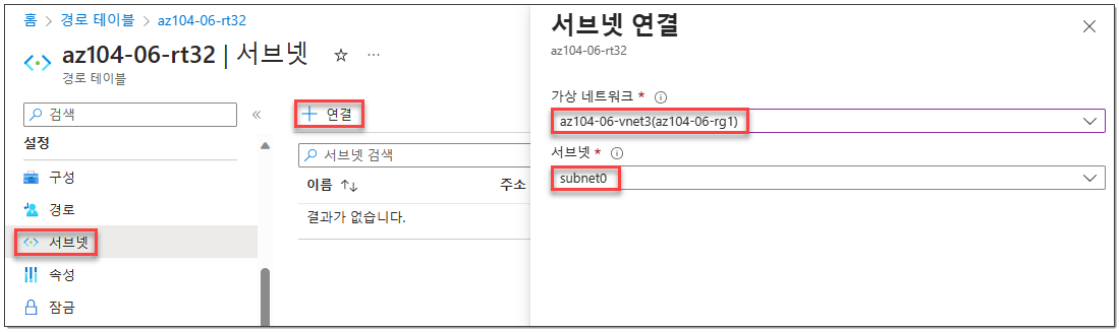


15. [경로 테이블] 블레이드로 다시 이동한 후 새로 만든 `az104-06-rt32` 경로 테이블을 클릭합니다.



16. [az104-06-rt32 경로 테이블] 블레이드의 [설정 - 경로]로 이동한 후 [추가]를 클릭합니다. [경로 추가]에서 다음과 같이 구성한 후 [추가]를 클릭합니다.
    - 경로 이름: az104-06-route-vnet3-to-vnet2
    - 대상 주소 접두사: IP 주소
    - 대상 IP 주소/CIDR 범위: 10.62.0.0/20
    - 다음 홉 형식: 가상 어플라이언스
    - 다음 홉 주소: 10.60.0.4

17. [az104-06-rt32 경로 테이블] 블레이드의 [설정 - 서브넷]으로 이동한 후 [연결]을 클릭합니다. [서브넷 연결] 창에서 아래와 같이 구성한 후 [확인]을 클릭합니다.
    - 가상 네트워크: az104-06-vnet3(az104-06-rg1)
    - 서브넷: subnet0



18. Azure 포털의 검색창에서 "Network Watcher"를 검색하여 클릭합니다. [Network Watcher] 블레이드의 [네트워크 진단 도구 - 연결 문제 해결]로 이동한 후 아래와 같이 구성하고 [선택]을 클릭합니다.
    - [소스 - Resource group]: az104-06-rg1
    - [소스 - 원본 유형]: 가상 머신
    - [소스 - 가상 머신]: az104-06-vm2
    - [대상 주소 - 대상 유형]: 수동으로 지정
    - [대상 주소 - URI, FQDN 또는 IP 주소]: az104-06-vm3의 프라이빗 IP 주소인 "10.63.0.4"를 입력

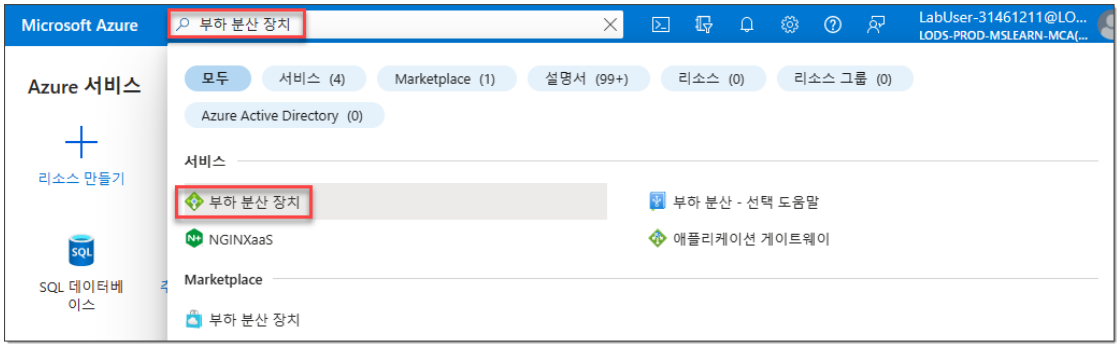
- [프로브 설정 - 프로토콜]: TCP
- [프로브 설정 - 대상 포트]: 3389
- [연결 진단 - 진단 테스트]: 모두 선택

19. 테스트 결과가 "연결 가능"으로 표시되는 것을 확인합니다. 네트워크 경로를 확인하면 트래픽은 `az104-06-nic0` 네트워크 어댑터에 할당된 `10.60.0.4`를 통해 라우팅된 것을 확인할 수 있습니다. 만약 "연결 가능"으로 표시되지 않는다면 `az106-06-vm0` 가상 머신을 재시작합니다.
    - 스포크 네트워크 간의 트래픽은 이제 허브 가상 네트워크에 있는 가상 머신을 통해 라우팅되기 때문에 이는 예상되는 결과입니다.
    - [토폴로지 보기] 탭을 클릭하여 네트워크 토폴로지도 확인해 봅니다.

TASK 05. Azure Load Balancer 구현

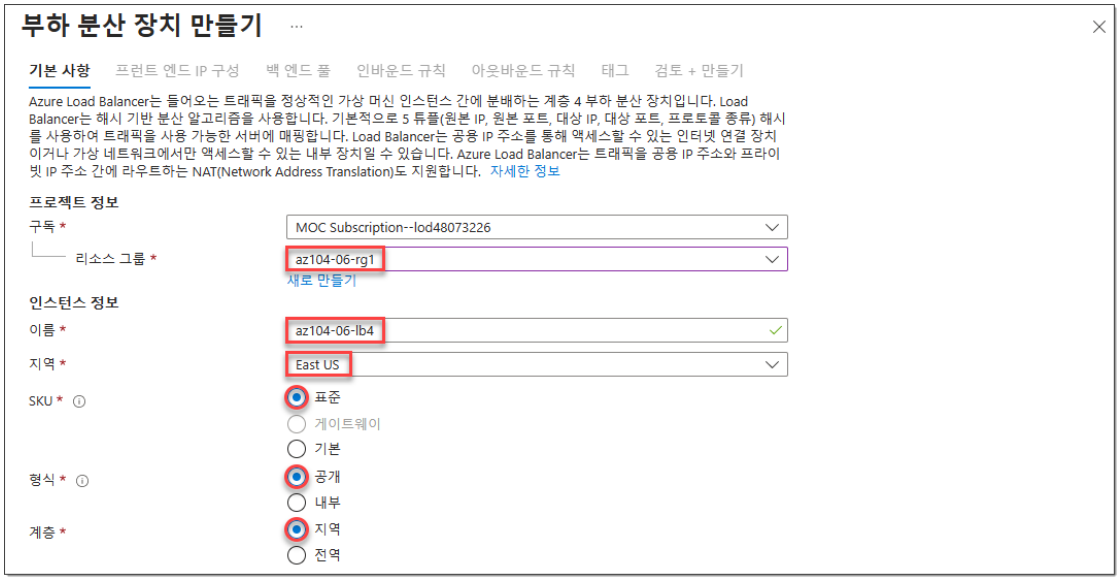
이 작업에서는 허브 가상 네트워크에 있는 두 대의 Azure 가상 머신 앞에 Azure Load Balancer를 구현합니다.

1. Azure 포털의 검색창에서 "부하 분산 장치"를 검색한 후 클릭합니다.

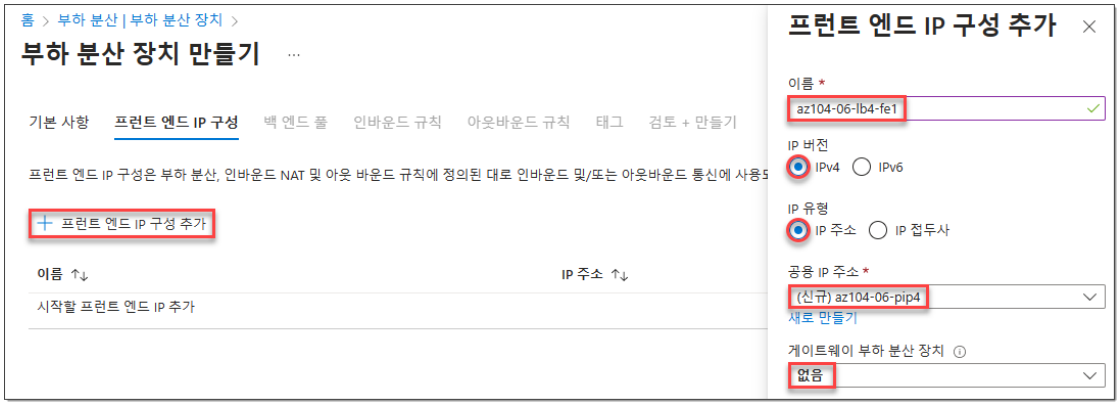


2. [부하 분산 장치] 블레이드의 [부하 분산 서비스 - 부하 분산 장치]에서 [만들기]를 클릭합니다.

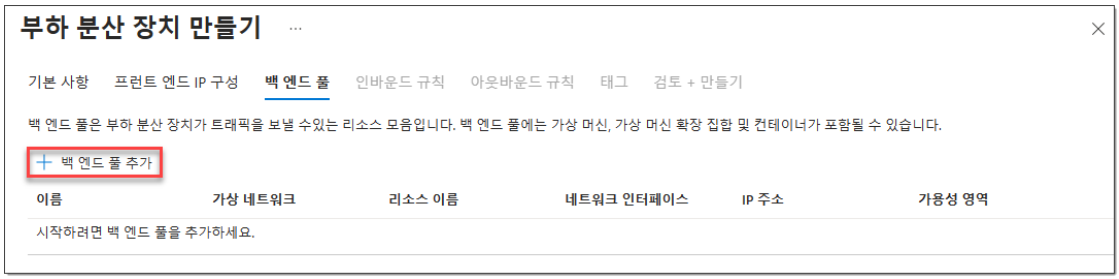
3. [부하 분산 장치 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성하고 [다음]을 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: az104-06-rg1
   - [인스턴스 정보 - 이름]: az104-06-lb4
   - [인스턴스 정보 - 지역]: East US
   - [인스턴스 정보 - SKU]: 표준
   - [인스턴스 정보 - 형식]: 공개
   - [인스턴스 정보 - 계층]: 지역



4. [프런트 엔드 IP 구성] 탭에서 [프런트 엔드 IP 구성 추가]를 클릭한 후 [프런트 엔드 IP 주소 추가] 창에서 다음과 같이 구성하고 [추가]를 클릭합니다. 프런트 엔드 IP 구성이 추가된 것을 확인하고 [다음]을 클릭합니다.
   - 이름: az104-06-lb4-fe1
   - IP 버전: IPv4
   - IP 유형: IP 주소
   - 공용 IP 주소: "새로 만들기"를 클릭한 후 이름은 "az104-06-pip4", 가용성 영역은 "영역 없음"을 선택하고 [확인]을 클릭합니다.
   - 게이트웨이 부하 분산 장치: 없음



5. [백 엔드 풀] 탭에서 [백 엔드 풀 추가]를 클릭합니다.

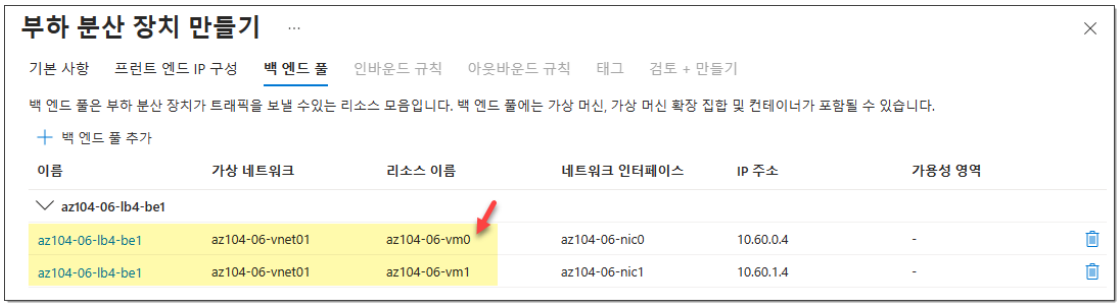


6. [백 엔드 풀 추가]에서 다음과 같이 구성한 후 [저장]을 클릭합니다.

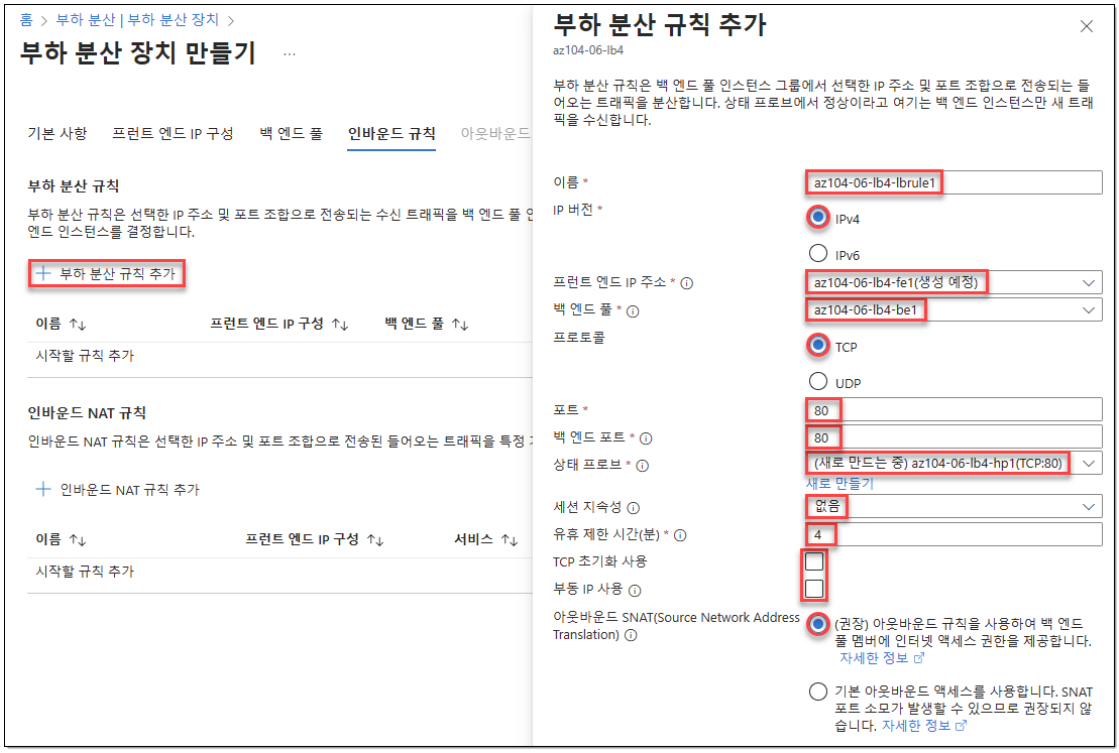
Microsoft

- 이름: az104-06-lb4-be1
- 가상 네트워크: az104-06-vnet01(az104-06-rg1)
- 백 엔드 풀 구성: NIC
- [IP 구성]에서 [추가]를 클릭합니다. [백 엔드 풀에 IP 구성 추가]에서 `az104-06-vm0`, `az104-06-vm1` 가상 머신을 선택하고 [추가]를 클릭합니다.

7. [백 엔드 풀] 탭에서 아래와 같이 두 대의 가상 머신이 구성된 것을 확인한 후 [다음]을 클릭합니다.



8. [인바운드 규칙] 탭에서 [부하 분산 규칙 추가]를 클릭합니다. [부하 분산 규칙 추가] 창에서 다음과 같이 구성한 후 [추가]를 클릭합니다.
   - 이름: az104-06-lb4-lbrule1
   - IP 버전: IPv4
   - 프런트 엔드 IP 주소: az104-06-lb4-fe1
   - 백 엔드 풀: az104-06-lb4-be1
   - 프로토콜: TCP
   - 포트: 80
   - 백 엔드 포트: 80
   - 상태 프로브: "새로 만들기"를 클릭합니다. [상태 프로브 추가]에서 이름 `"az104-06-lb4-hp1"`, 프로토콜 `"TCP"`, 포트 `"80"`, 간격 `"5"`를 입력한 후 [확인]을 클릭합니다.
   - 세션 지속성: 없음
   - 유휴 제한 시간(분): 4
   - TCP 초기화: 선택하지 않습니다.
   - 부동 IP 사용: 선택하지 않습니다.
   - 아웃바운드 SNAT(Source Network Address Translation): (권장) 아웃바운드 규칙을 사용하여 백 엔드 풀 멤버에 인터넷 액세스 권한을 제공합니다.



9. [인바운드 규칙] 탭에서 [인바운드 NAT 규칙 추가]를 클릭합니다.

10. [인바운드 NAT 규칙 추가] 창에서 아래와 같이 구성한 후 [추가]를 클릭합니다.
    - 이름: az104-06-lb4-natrule1
    - 형식: 백 엔드 풀
    - 대상 백 엔드 풀: az104-06-lb4-be1
    - 프런트 엔드 IP 주소: az104-06-lb4-fe1
    - 프런트 엔드 포트 범위 시작: 8000
    - 백 엔드 풀의 최대 컴퓨터 수: 10
    - 백 엔드 포트: 3389
    - 프로토콜: TCP
    - TCP 초기화 사용: 선택하지 않습니다.
    - 유휴 제한 시간(분): 4
    - 부동 IP 사용: 선택하지 않습니다.

11. [인바운드 규칙]에서 다음과 같이 부하 분산 규칙과 인바운드 NAT 규칙이 추가된 것을 확인하고 [다음]을 클릭합니다.

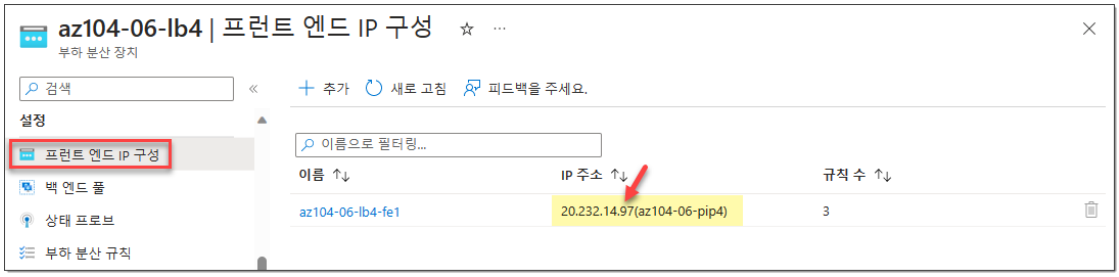
12. [아웃바운드 규칙] 탭에서 [아웃바운드 규칙 추가]를 클릭합니다.

13. [아웃바운드 규칙 추가]에서 다음과 같이 구성한 후 [추가]를 클릭합니다.
    - 이름: az104-06-lb4-snatrule1
    - IP 버전: IPv4
    - 프런트 엔드 IP 주소: az104-06-lb4-fe1
    - 프로토콜: All

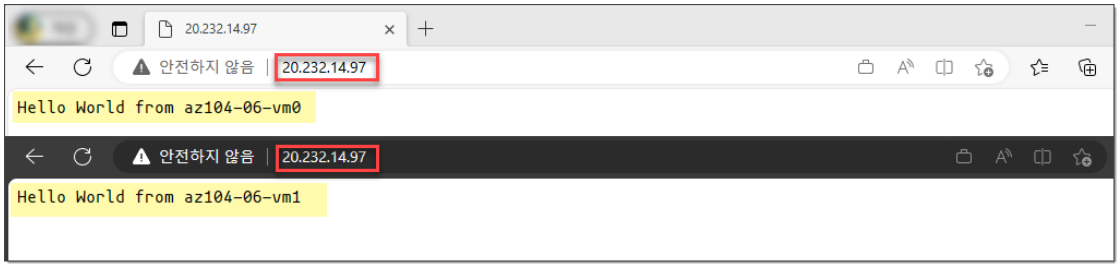
- 유휴 제한 시간(분): 4
- TCP 재설정: 사용
- 백 엔드 풀: az104-06-lb4-be1
- [포트 할당 - 포트 할당]: 아웃바운드 포트 수 수동 선택
- [포트 할당 - 선택 기준]: 백 엔드 인스턴스의 최대 수
- [포트 할당 - 인스턴스당 포트 수]: 10

14. [아웃바운드 규칙] 탭에서 다음과 같이 아웃바운드 규칙이 추가된 것을 확인하고 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

15. 배포가 완료되면 [리소스로 이동]을 클릭합니다. [부하 분산 장치] 블레이드의 [설정 - 프런트 엔드 IP 구성]으로 이동한 후 표시되는 공용 IP 주소를 클립보드에 복사합니다.



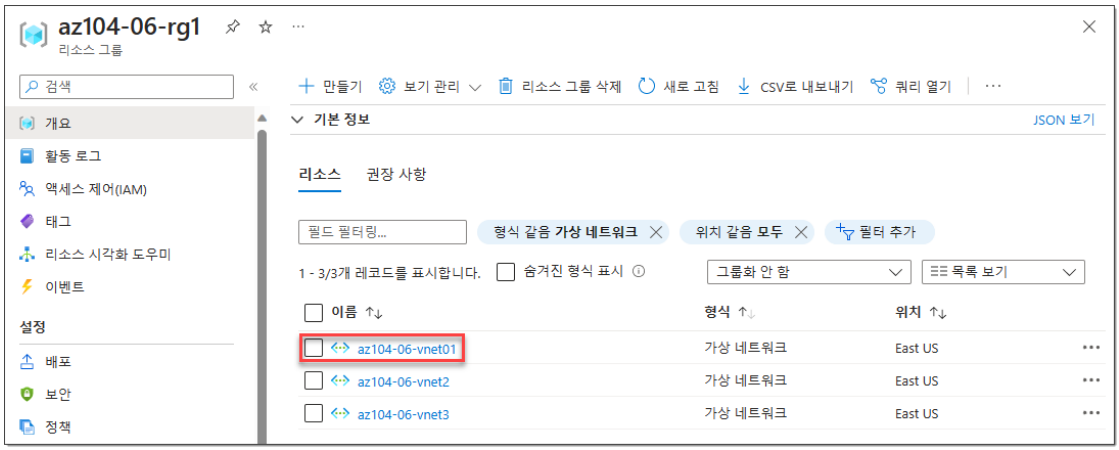
16. 브라우저에서 새 탭을 열고 위에서 메모한 공용 IP 주소에 액세스합니다. InPrivate 브라우저를 하나 더 열고 동일한 공용 IP 주소에 액세스합니다. 아래와 같이 서로 다른 두 대의 웹 서버에서 응답을 받습니다.



TASK 06. Azure Application Gateway 구현

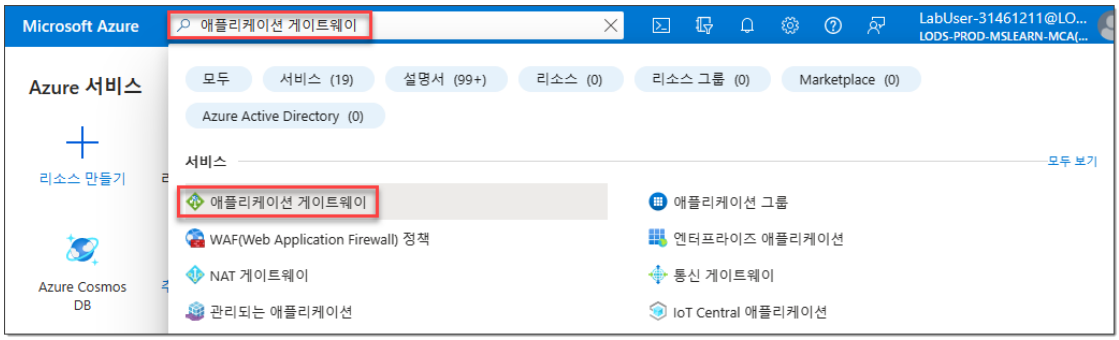
이 작업에서는 스포크 가상 네트워크에 있는 두 대의 Azure 가상 머신 앞에 Azure Application Gateway를 구현합니다.

1. Azure 포털에서 [`az104-06-rg1` 리소스 그룹] 블레이드로 이동한 후 `az104-06-vnet01` 가상 네트워크 리소스를 클릭합니다.



2. [`az104-06-vnet01` 가상 네트워크] 블레이드의 [설정 - 서브넷]으로 이동한 후 메뉴에서 [서브넷]을 클릭합니다. [서브넷 추가] 창에서 서브넷 이름은 "`subnet-appgw`", 서브넷 주소 범위는 "`10.60.3.224/27`"을 입력한 후 [저장]을 클릭합니다.
   - 이 서브넷은 Azure Application Gateway 인스턴스에서 사용합니다. Application Gateway는 전용 서브넷으로 `/27` 이상의 서브넷이 필요합니다.

3. Azure 포털의 검색창에서 "애플리케이션 게이트웨이"를 검색한 후 클릭합니다.



4. [부하 분산] 블레이드의 [부하 분산 서비스 - Application Gateway]로 이동한 후 메뉴에서 [만들기]를 클릭합니다.

5. [애플리케이션 게이트웨이 만들기] 블레이드의 [기본 사항] 탭에서 다음과 같이 구성한 후 [다음]을 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: az104-06-rg1
   - [인스턴스 정보 - 게이트웨이 이름]: az104-06-appgw5
   - [인스턴스 정보 - 지역]: East US
   - [인스턴스 정보 - 계층]: WAF V2
   - [인스턴스 정보 - 자동 크기 조정]: 아니요
   - [인스턴스 정보 - 인스턴스 수]: 2
   - [인스턴스 정보 - 가용성 영역]: 없음
   - [인스턴스 정보 - HTTP2]: 사용 안 함

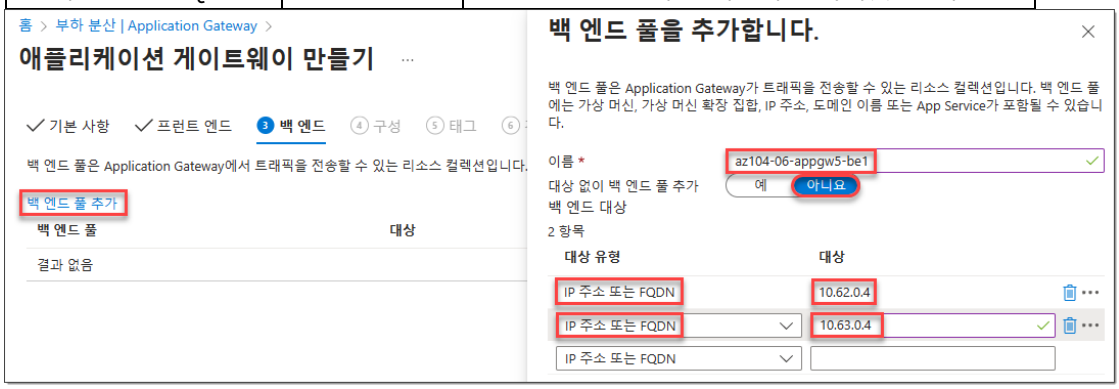
- [인스턴스 정보 - WAF 정책]: "새로 만들기" 링크를 클릭합니다. [웹 애플리케이션 방화벽 정책 만들기]에서 이름에 "az104-06-waf-policy"를 입력하고 "봇 보호 추가" 옵션을 선택한 후 [확인]을 클릭합니다.
- [가상 네트워크 구성 - 가상 네트워크]: az104-06-vnet01
- [가상 네트워크 구성 - 서브넷]: subnet-appgw(10.60.3.224/27)

6. [프런트 엔드] 탭에서 아래와 같이 구성한 후 [다음]을 클릭합니다.
   - 프런트 엔드 IP 형식: 공용
   - 공용 IP 주소: "새로 추가"를 클릭한 후 [공용 IP 추가] 창에서 이름에 "az104-06-pip5"를 입력한 후 [확인]을 클릭합니다.

7. [백 엔드] 탭에서 "백 엔드 풀 추가"를 클릭합니다. [백 엔드 풀을 추가합니다.] 창에서 아래와 같이 구성한 후 [추가]를 클릭합니다. [백 엔드] 탭에서 백 엔드 풀이 추가된 것을 확인하고 [다음]을 클릭합니다.
   - 이름: az104-06-appgw5-be1
   - 대상 없이 백 엔드 풀 추가: 아니요

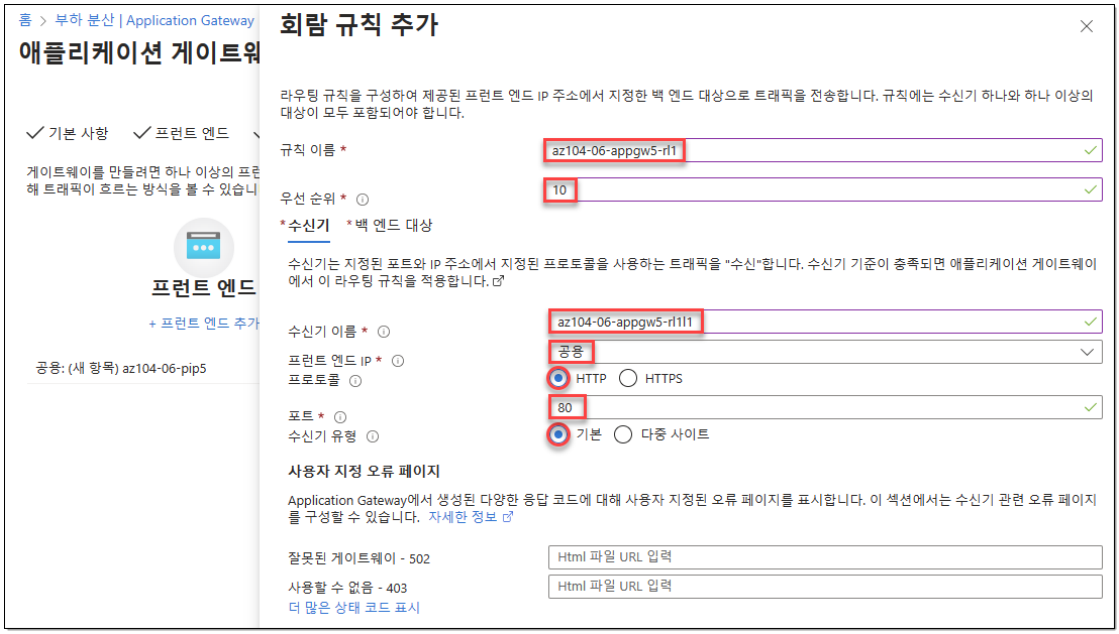
- 백 엔드 대상

대상 유형	대상	설명
IP 주소 또는 FQDN	10.62.0.4	az104-06-vm2 가상 머신의 프라이빗 IP 주소
IP 주소 또는 FQDN	10.63.0.4	az104-06-vm3 가상 머신의 프라이빗 IP 주소

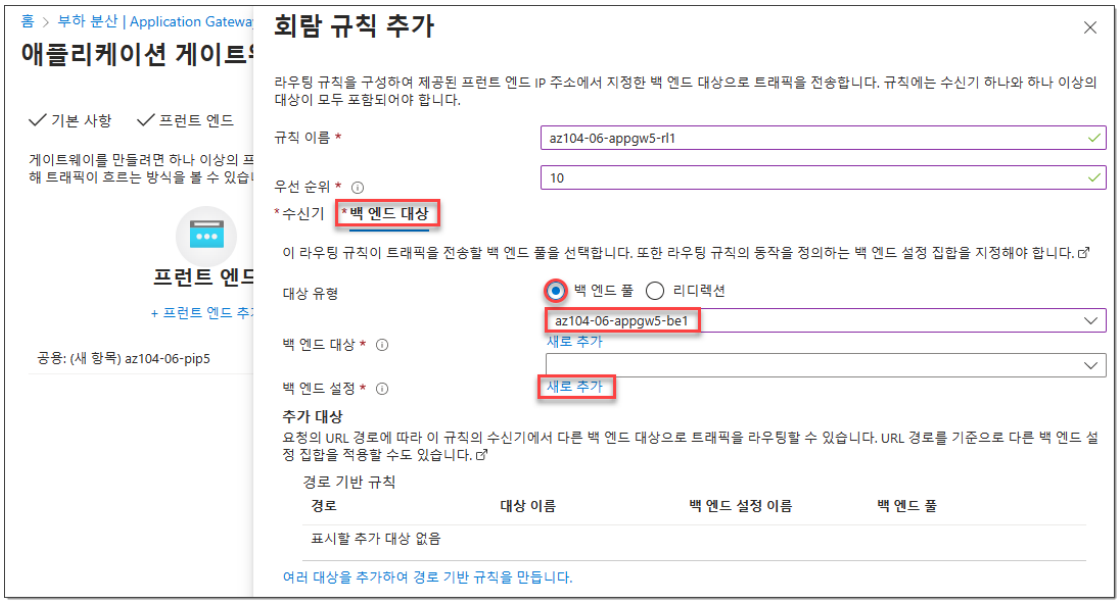


8. [구성] 탭에서 [회람 규칙 추가]를 클릭합니다. 회람 규칙은 라우팅 규칙을 말합니다.

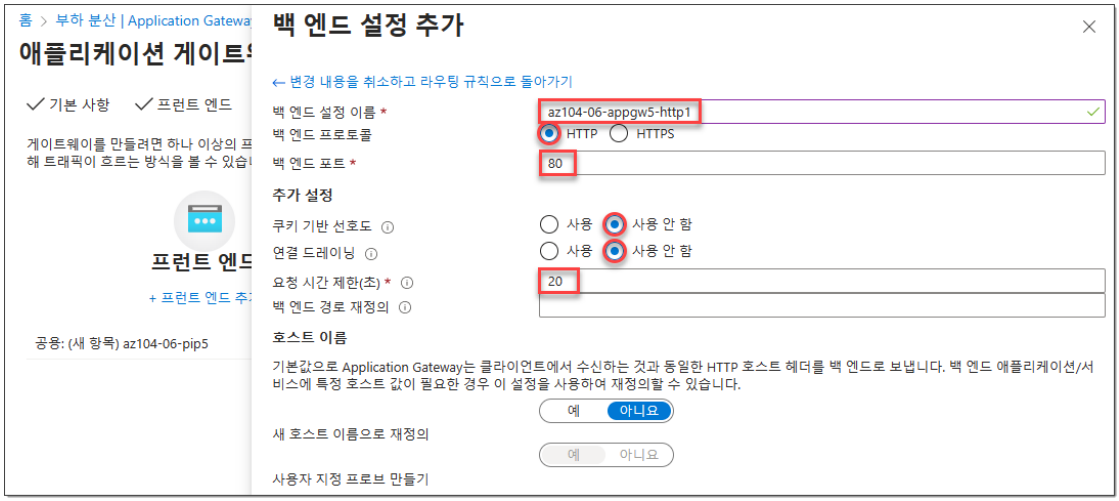
9. [회람 규칙 추가] 창의 [수신기] 탭에서 다음과 같이 구성합니다.
   - 규칙 이름: az104-06-appgw5-rl1
   - 우선 순위: 10
   - 수신기 이름: az104-06-appgw5-rl1l1
   - 프런트 엔드 IP: 공용
   - 프로토콜: HTTP
   - 포트: 80
   - 수신기 유형: 기본
   - 사용자 지정 오류 페이지: 아무런 값도 입력하지 않습니다.



10. [회람 규칙 추가]의 [백 엔드 대상] 탭에서 다음과 같이 구성한 후 백 엔드 설정에서 "새로 추가"를 클릭합니다.
    - 대상 유형: 백 엔드 풀
    - 백 엔드 대상: az104-06-appgw5-be1



11. [백 엔드 설정 추가] 창에서 다음과 같이 구성한 후 [추가]를 클릭합니다.
    - 백 엔드 설정 이름: az104-06-appgw5-http1
    - 백 엔드 프로토콜: HTTP
    - 백 엔드 포트: 80
    - [추가 설정]: 모드 기본값을 사용합니다.
    - [호스트 이름]: 모두 기본값을 사용합니다.



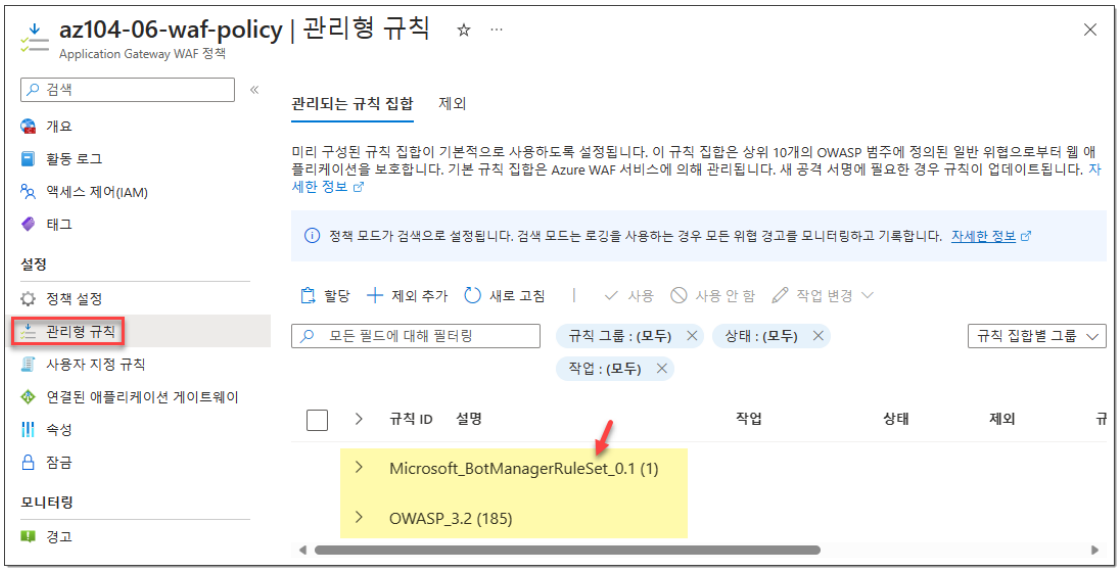
12. [회람 규칙 추가] 창에서 [추가]를 클릭합니다. [애플리케이션 게이트웨이 만들기] 블레이드의 [구성] 탭에서 회람 규칙이 추가된 것을 확인하고 [다음]을 클릭합니다.

13. [태그] 탭에서 [다음]을 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다. 리소스가 생성되면 [리소스로 이동]을 클릭합니다.
14. [`az104-06-appgw5` 애플리케이션 게이트웨이] 블레이드의 [개요]에서 프런트 엔드 공용 IP 주소를 클립보드에 복사합니다.

15. 브라우저에서 새 탭을 열고 위에서 복사한 IP 주소에 액세스합니다. `az104-06-vm2` 혹은 `az104-06-vm3`의 페이지가 표시되는 것을 확인합니다.

16. [`az104-06-rg1` 리소스 그룹] 블레이드로 이동한 후 `az104-06-waf-policy` Application Gateway WAF 정책 리소스를 클릭합니다.

17. [`az104-06-waf-policy` Application Gateway WAF 정책] 블레이드에서 표시되는 WAF 정책을 검토합니다.

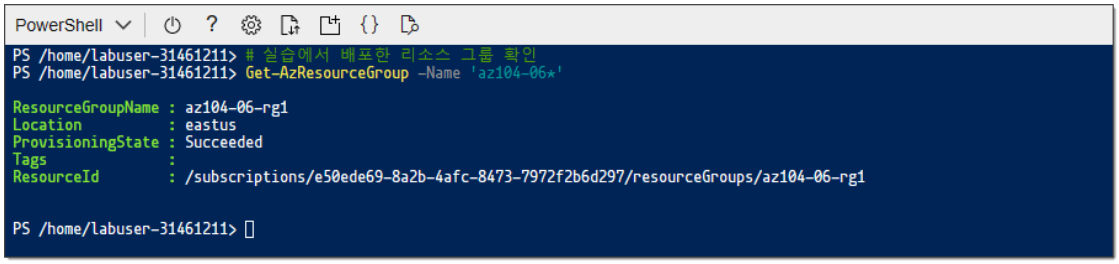


18. 실습에서 구성한 것처럼 여러 가상 네트워크의 가상 머신을 애플리케이션 게이트웨이의 대상으로 지정하는 것은 일반적인 구성은 아닙니다. 하지만 애플리케이션 게이트웨이가 동일한 가상 네트워크의 가상 머신 간 부하를 분산하는 Azure Load Balancer와 달리 여러 가상 네트워크(다른 Azure 지역 혹은 Azure 외부의 엔드포인트 포함)의 가상 머신을 대상으로 할 수 있다는 것을 확인할 수 있습니다.

TASK 07. 리소스 정리

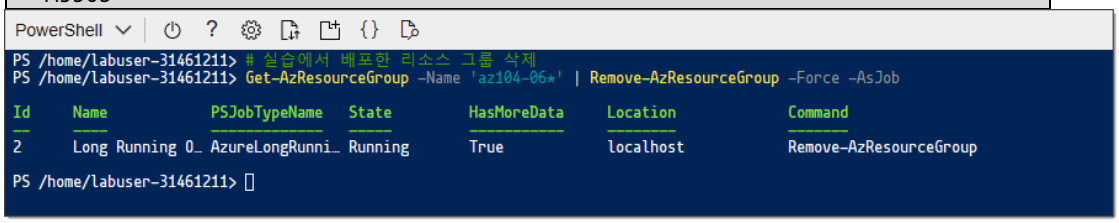
1. [Cloud Shell]에서 PowerShell을 열고 다음 명령을 실행하여 이 실습에서 만든 모든 리소스 그룹을 확인합니다.

```
# 실습에서 배포한 리소스 그룹 확인
Get-AzResourceGroup -Name 'az104-06*'
```



2. [Cloud Shell]에서 다음 명령을 실행하여 실습에서 만든 모든 리소스 그룹을 삭제합니다. 이 명령은 `-AsJob` 매개 변수로 인해 비동기적으로 실행되므로 PowerShell 세션 내에서 다른 PowerShell 명령을 즉시 실행할 수 있지만 리소스 그룹이 실제로 삭제될 때까지는 몇 분 정도 걸립니다.

```
# 실습에서 배포한 리소스 그룹 삭제
Get-AzResourceGroup -Name 'az104-06*' | Remove-AzResourceGroup -Force `
 -AsJob
```



Microsoft