

가상 네트워크(VNet) 생성 후 네트워크 보안 그룹(NSG)을 통해 네트워크 트래픽 필터링(NIC에 연결)

주신영 bit1010@live.com

지역은 계정에 제한이 없다면 Korea Central을 선택합니다.



동일한 가상네트워크(VNet)에 포함된 가상 머신은 모든 포트를 통해 서로 통신할 수 있습니다.



네트워크 보안 그룹은 가상머신의 네트워크 인터페이스 카드(NIC)에 직접 연결하거나 서브넷에 연결해서 사용할 수 있습니다.

이번 실습에서는 네트워크 보안 그룹을 가상머신의 네트워크 인터페이스 카드(NIC)에 연결해서 사용해보겠습니다.

가상 네트워크 만들기

이전 실습에서 가상머신 생성 시 VNet은 기본 설정으로 생성되었습니다. 가상머신은 VNet 없이 생성이 안됩니다.

1. 포털에서 **virtual network**를 검색하고 선택합니다.
2. 가상 네트워크 페이지에서 **만들기**를 선택합니다.
3. 가상 네트워크 만들기 화면의 **기본 사항** 탭에서 다음 정보를 입력하거나 선택합니다.
 - **리소스 그룹**: 새로 만들기를 선택한 다음, 리소스 그룹 이름을 *myVNetNSGRG*로 지정합니다.

* 리소스 그룹이 생성되어 있으면 선택합니다.

- **가상 네트워크 이름:** VNet을 입력합니다.

가상 네트워크 만들기 ...

[기본 사항](#) [IP 주소](#) [보안](#) [태그](#) [검토 + 만들기](#)

VNet(Azure Virtual Network)은 Azure에서 프라이빗 네트워크의 기본 빌딩 블록입니다. VNet을 사용하면 Azure Virtual Machines(VM)과 같은 다양한 유형의 Azure 리소스가 서로 통신하거나 인터넷 및 온-프레미스 네트워크와 안전하게 통신할 수 있습니다. VNet은 데이터 센터에서 작동하는 전통적인 네트워크와 유사하지만, 확장, 가용성, 격리 등 Azure 인프라의 추가 혜택을 제공합니다. [가상 네트워크에 대한 자세한 정보](#)

프로젝트 정보

구독 * ⓘ

Microsoft Azure 스폰서십

리소스 그룹 * ⓘ

(신규) myVNetRG

[새로 만들기](#)

인스턴스 정보

이름 *

VNet

지역 *

한국 중부

4. 페이지 아래쪽에서 다음: **IP 주소**를 선택합니다.

5. **IP 주소** 탭의 **IPv4 주소 공간**에서 10.0.0.0/16을 입력합니다.

* 주소공간이 변경되면 기본 설정된 서브넷이 삭제됩니다.

6. **서브넷 추가**를 선택합니다.

7. **서브넷 추가** 화면에서 다음 정보를 입력한 다음, **추가**를 선택합니다.

- **서브넷 이름:** default
- **서브넷 주소 범위:** 10.0.0.0/24

- 화면 아래쪽에서 검토 + 만들기 를 선택하고 유효성 검사가 통과되면 만들기를 선택합니다.

가상 머신 만들기

가상 네트워크에 *myVMWeb* 및 *myVMMgmt* 라는 두 개의 VM을 만듭니다.

- 포털에서 가상 머신을 검색하고 선택합니다.
- 가상 머신 페이지에서 만들기를 선택하고 Azure 가상 머신을 선택합니다.
- 가상 머신 만들기 화면의 기본 사항 탭에서 다음 값을 입력하거나 선택합니다.

- **리소스 그룹:** 가상 네트워크와 동일하게 선택
 * 리소스 그룹이 생성되어 있으면 선택합니다..
- **가상 머신 이름:** *myVMWeb*을 입력합니다.
- **가용성 옵션:** **인프라 중복이 필요하지 않음**을 선택합니다.
- **이미지:** **Windows Server 2022 Datacenter - x64 Gen2**를 선택합니다.
- **크기:** 기본값을 적용하거나 드롭다운하여 크기를 선택합니다.
- **사용자 이름, 암호 및 암호 확인:** VM에 대한 관리자 사용자 이름 및 암호를 입력합니다.
- **공용 인바운드 포트:** **HTTP(80)**을 선택합니다.

기본 사항 디스크 네트워킹 관리 Monitoring 고급 태그 검토 + 만들기

Linux 또는 Windows를 실행하는 가상 머신을 만듭니다. Azure Marketplace에서 이미지를 선택하거나 고유한 사용자 지정 이미지를 사용합니다. [기본] 탭을 완료하고 [검토 + 만들기]하여 기본 매개 변수로 가상 머신을 프로비전하거나, 전체 사용자 지정에 대해 각 탭을 검토합니다. [자세한 정보](#)

프로젝트 정보
 배포된 리소스와 비용을 관리할 구독을 선택합니다. 폴더 같은 리소스 그룹을 사용하여 모든 리소스를 정리 및 관리합니다.

구독 * ① Microsoft Azure 스폰서십 ▼

리소스 그룹 * ① ((신규) myVNetRG) ▼
[새로 만들기](#)

인스턴스 정보

가상 머신 이름 * ① myVMWeb ✓

지역 * ① ((Asia Pacific) 한국 중부) ▼

가용성 옵션 ① 인프라 중복이 필요하지 않습니다. ▼

보안 유형 ① 표준 ▼

이미지 * ① Windows Server 2022 Datacenter: Azure Edition - x64 Gen2 ▼
[모든 이미지 보기](#) | VM 생성 구성

VM 아키텍처 ①

☐ Arm64

☒ x64

i Arm64는 선택한 이미지에서 지원되지 않습니다.

4. 페이지 맨 위에 있는 **네트워킹** 탭을 선택합니다.
5. **네트워킹** 페이지에서 다음 값을 입력하거나 선택합니다.

- **가상 네트워크:** 이전에 생성한 **VNet** 을 선택합니다.
VNet이 여러 개일 경우 리소스 그룹 이름도 같이 확인합니다.
- **서브넷:** **default** 을 선택합니다.
- **공용 IP:** 자동으로 생성된 IP를 그대로 사용합니다. (**새로 만드는 중**) myVMWeb-ip

* NIC 네트워크 보안 그룹을 없음으로 만들 경우 현재 구성으로는 가상머신은 인터넷으로 연결 할 수 없습니다.

기본 사항 디스크 **네트워킹** 관리 Monitoring 고급 태그 검토 + 만들기

NIC(네트워크 인터페이스 카드) 설정을 구성하여 가상 머신에 대한 네트워크 연결을 정의합니다. 보안 그룹 규칙을 사용하여 포트, inbound 및 아웃바운드 연결을 제어하거나 기존 부하 분산 솔루션 뒤에 배치할 수 있습니다. [자세한 정보](#)

네트워크 인터페이스

가상 머신을 만들면 네트워크 인터페이스가 만들어집니다.

가상 네트워크 * ① (새로 만드는 중) VNet
[새로 만들기](#)

서브넷 * ① (새로 만드는 중) default(10.1.0.0/24)

공용 IP ① (새로 만드는 중) myVMWeb-ip
[새로 만들기](#)

NIC 네트워크 보안 그룹 ① ☐ 없음 ☒ 기본 ☐ 고급

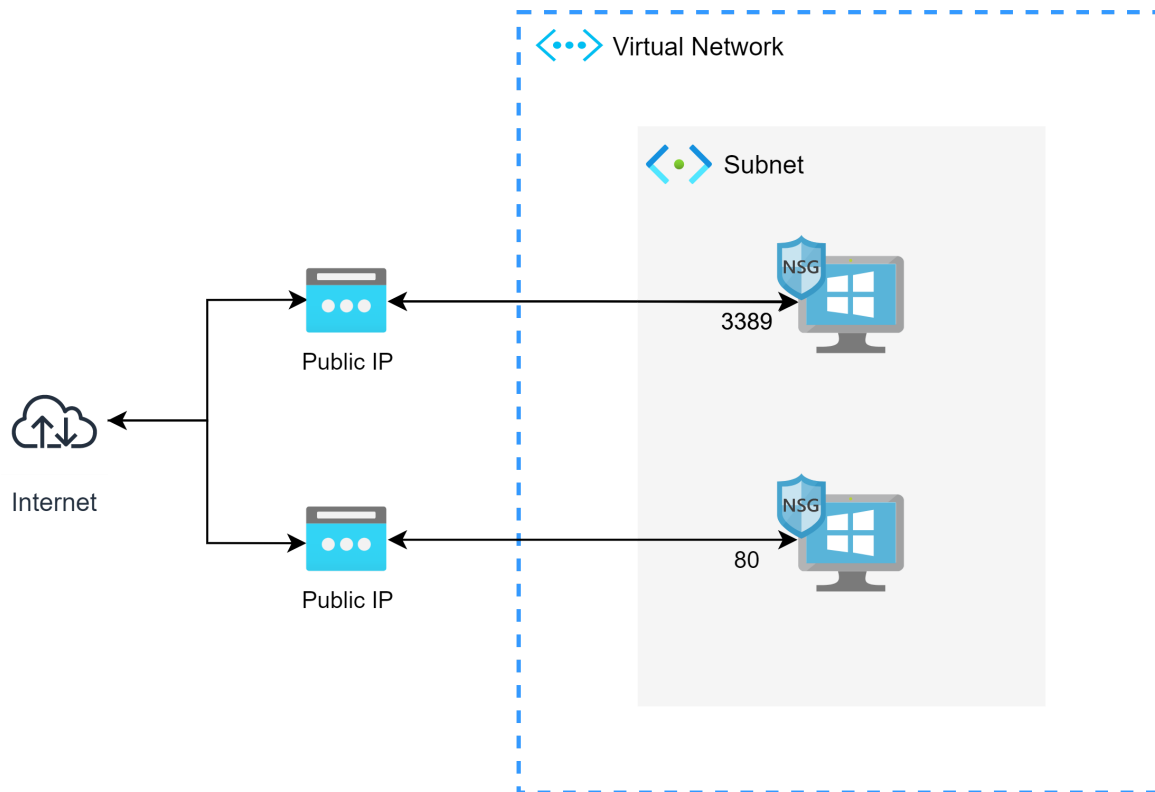
공용 inbound 포트 * ① ☐ 없음 ☒ 선택한 포트 허용

inbound 포트 선택 * HTTP (80)

6. 다른 설정을 적용하고 **검토 + 만들기**를 선택합니다. 설정을 검토한 다음, **만들기**를 선택합니다.
7. VM 만들기가 완료되면 **다른 VM 만들기** 를 선택하여 **두 번째 VM**을 만들 수 있습니다.
리소스 그룹: 이전에 생성한 리소스 그룹 선택합니다.
가상 머신 이름: myVMMgmt을 입력합니다.
공용 inbound 포트: RDP(3389)을 선택합니다.

다른 설정은 동일하게 적용하고 **검토 + 만들기**를 선택합니다. 설정을 검토한 다음, **만들기**를 선택합니다.

리소스 그룹에 생성된 리소스 확인



가상머신 생성시 **NIC 네트워크 보안 그룹**을 기본으로 선택했으므로 네트워크 보안 그룹(NSG)이 각각 1개씩 생성됐습니다. 고급으로 변경해서 기존 네트워크 보안 그룹을 선택할 수도 있습니다.

가상네트워크인 VNet 리소스로 이동하여 주소 공간과 서브넷을 확인합니다.

myVMMgmt | 네트워킹

가상 머신

검색

개요 활동 로그 액세스 제어(IAM) 태그 문제 진단 및 해결 설정

네트워킹 연결 Windows Admin Center(미리 보기) 디스크 크기 클라우드용 Microsoft Defender Advisor 권장 사항

myvmgmt708

IP 구성

ipconfig1 (기본)

네트워크 인터페이스: myvmgmt708 유효한 보안 규칙 VM 연결 문제 해결 토크로지

가상 네트워크/서브넷: VNet/default NIC 공용 IP: 20.249.22.146 NIC 프라이빗 IP: 10.1.0.5 가속화된 네트워킹: 사용

인바운드 포트 규칙 아웃바운드 포트 규칙 애플리케이션 보안 그룹 부하 분산

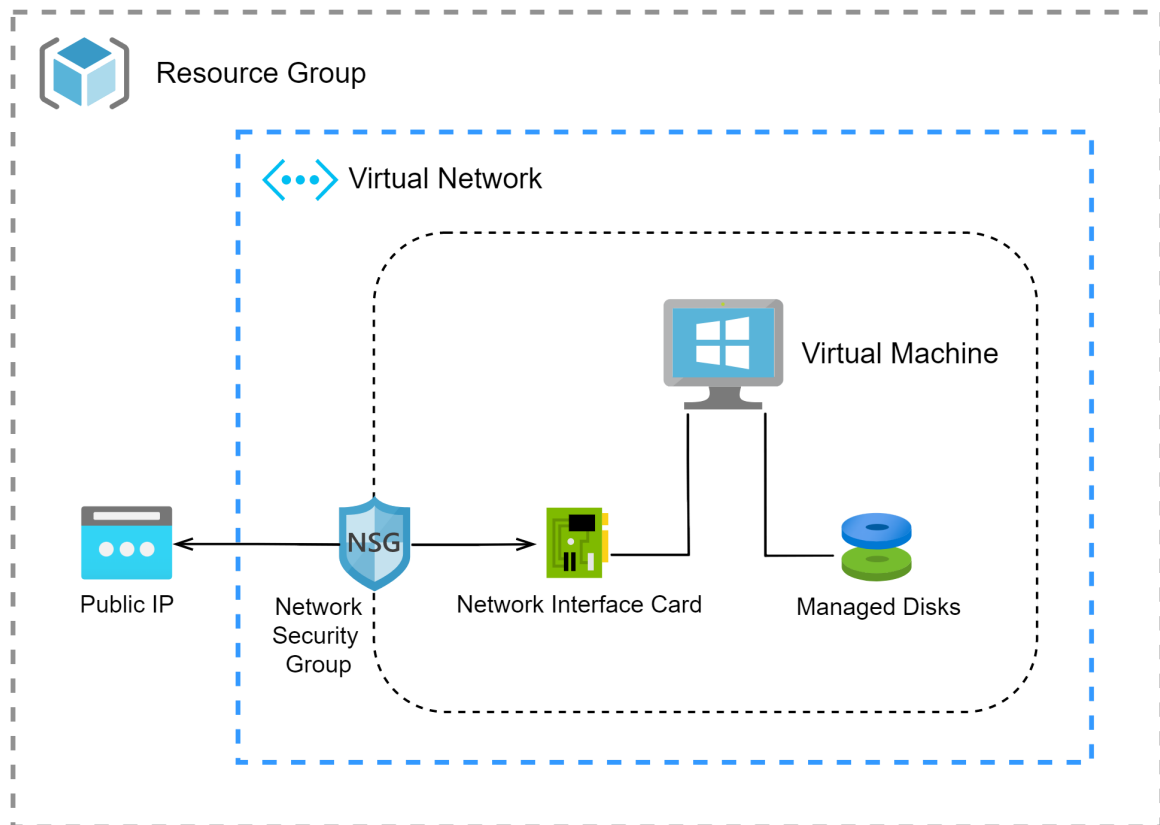
네트워크 보안 그룹 myVMMgmt-nsg (네트워크 인터페이스에 연결됨: myvmgmt708)

영향 0개 서버넷, 1개 네트워크 인터페이스

인바운드 포트 규칙 추가

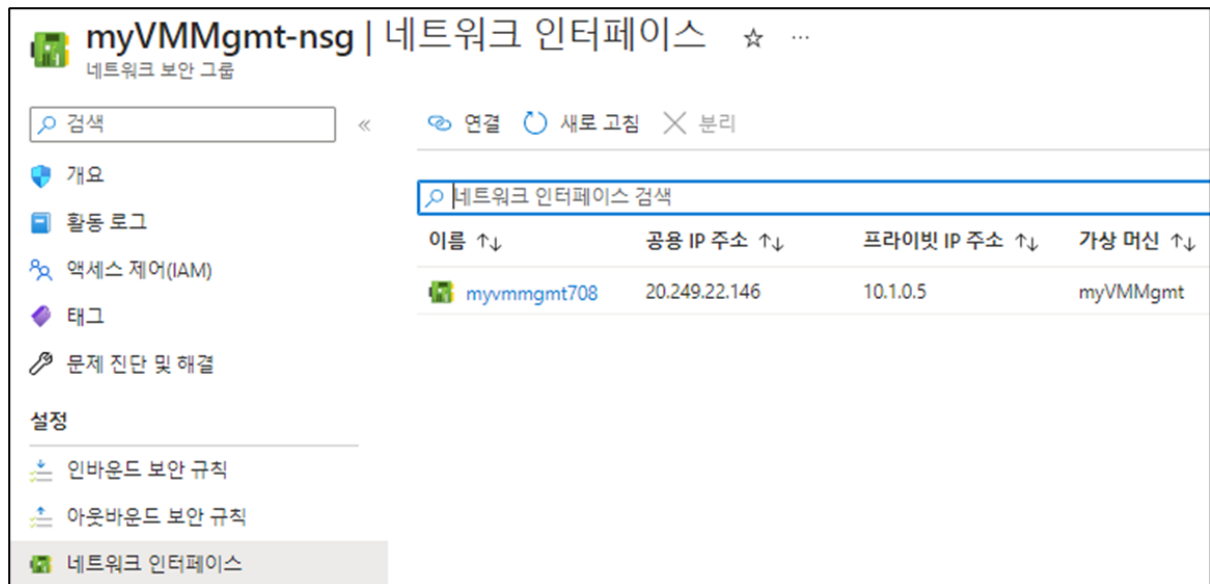
우선 순위	이름	포트	프로토콜	소스	대상 주소	작업
300	RDP	3389	TCP	모두	모두	허용
65000	AllowVnetInBound	모두	모두	VirtualNetwork	VirtualNetwork	허용
65001	AllowAzureLoadBalance...	모두	모두	AzureLoadBalancer	모두	허용
65500	DenyAllInBound	모두	모두	모두	모두	거부

가상 머신의 설정 메뉴에서 **네트워킹**으로 들어가면 연결된 가상네트워크/서브넷, 네트워크 인터페이스, 네트워크 보안 그룹을 볼 수 있고 **인바운드/아웃바운드 포트**는 연결된 네트워크 보안 그룹의 설정된 정보입니다. 각 가상머신에서 확인해보면 각각 80과 3389가 인바운드 포트로 설정되어 있습니다.



현재 설정은 네트워크 인터페이스 카드(Network Interface Card, NIC)에 네트워크 보안 그룹(NSG)이 연결된 상태입니다.

myvmmgmt 네트워크 인터페이스를 선택하고 **설정에서 네트워크 보안 그룹**으로 이동하면 myVMMgmt-nsg가 선택되어 있는 걸 확인 할 수 있습니다.



myvmweb도 동일하게 확인 가능합니다.

해당 메뉴를 통해 다른 네트워크 보안 그룹을 선택 가능 하며 **네트워크 보안 그룹의 네트워크 인터페이스 메뉴**를 통해서도 가능합니다.

관리 서버로 접속하여 웹서버에 IIS설치

1. 포털 검색 상자에서 *myVMMgmt*를 검색합니다.
2. 개요 페이지에서 **연결** 단추를 선택한 다음 **RDP**를 선택합니다.
3. **RDP 파일 다운로드**를 선택합니다.
4. 다운로드한 rdp 파일을 열고 **연결**을 선택합니다. VM을 만들 때 지정한 사용자 이름과 암호를 입력합니다.
5. **확인**을 선택합니다.
6. 연결 프로세스 중에 인증서 경고를 받을 수 있습니다. 경고 메시지가 표시되면 **예** 또는 **계속**을 선택하여 연결을 계속합니다.
7. PowerShell 세션을 엽니다. 다음을 사용하여 **myVMWeb**에 연결합니다.

```
mstsc /v:myVmWeb
```

mstsc는 원격데스크탑의 실행파일 이름입니다.

로그인해서 접속합니다.



기본적으로 동일한 네트워크의 가상 머신은 모든 포트에 연결할 수 있으므로 myVMMgmt에서 myVMWeb으로의 RDP 연결이 성공합니다. 인터넷에서 모든 리소스의 인바운드 트래픽은 기본적으로 거부됩니다.

8. Microsoft IIS를 **myVMWeb** 가상 머신에 설치하려면 **myVMWeb** 가상 머신에서 PowerShell을 실행하여 다음 명령을 입력하고 IIS서버를 활성화 합니다.

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

9. 포털 검색 상자에서 **myVMWeb**을 검색합니다.

10. **myVMWeb**의 개요 페이지에서 VM의 **공용 IP 주소**를 복사합니다.

The screenshot shows the Azure portal interface for a virtual machine named 'myVMWeb'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Windows Admin Center (previ...), Disks, and Size. The main content area shows the 'Overview' page with an 'Advisor' section at the top indicating a disk encryption recommendation. Below this, the 'Essentials' section lists VM details: Resource group (myResourceGroup), Status (Running), Location (East US), Subscription (change), Subscription ID, and Tags (change). On the right, a table-like structure shows: Operating system (Windows (Windows Server 2019 Datacenter)), Size (Standard D2s v3 (2 vcpus, 8 GiB memory)), Public IP address (23.96.39.113, highlighted with a red box), Virtual network/subnet (myVNet/default), and DNS name (Configure).

11. 인터넷에서 **myVMWeb** 웹 서버에 액세스할 수 있는지 확인하기 위해 컴퓨터에서 인터넷 브라우저에서 해당 주소로 이동합니다.

VM 간 통신

1. **myVMMgmt**의 데스크톱에서 PowerShell을 엽니다.
2. `ping myVMWeb`를 입력합니다. 다음 메시지와 유사한 회신이 표시됩니다.

```
PS C:\Users\VM1> ping myVMWeb

Pinging VM2.ovvzzdczhbu5iczfvonhg2zrb.bx.internal.cloudapp.net with 32 bytes of data
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



ping은 ICMP(인터넷 제어 메시지 프로토콜)를 사용하기 때문에 실패합니다.
기본적으로 ICMP는 Windows 방화벽을 통해 허용되지 않습니다.

3. ICMP가 이 VM의 Windows 방화벽을 통해 인바운드 되도록 허용하려면 다음 명령을 입력합니다.

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

4. myVMWeb도 동일하게 연결하여 PowerShell에서 `ping myVMMgmt` 를 입력합니다
이번에는 myVMMgmt의 방화벽을 통해 ICMP를 허용했기 때문에 다음 메시지와 유사한 성공 회신이 표시됩니다.
반대로 myVMWeb에서도 ICMP를 허용하도록 설정하고 myVMMgmt에서 `ping myVMWeb` 을 입력합니다.

```
PS C:\Users\VM2> ping myVMWeb

Pinging VM1.e5p2dibbrqtejhq04lqrusvd4g.bx.internal.cloudapp.net [10.0.0.4] with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=2ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

5. myVMMgmt로 연결한 원격 데스크탑을 닫습니다.

리소스 정리

가상 네트워크 및 VM 사용을 완료하면 리소스 그룹 및 모든 해당 리소스를 삭제할 수 있습니다.

1. Azure Portal에서 **리소스 그룹**을 검색하고 선택합니다.
2. **리소스 그룹** 페이지에서 **myVNetNSGRG** 리소스 그룹을 선택합니다.
3. **myVNetNSGRG** 페이지에서 리소스 그룹에 포함된 모든 리소스를 확인합니다. 페이지 위쪽에서 **리소스 그룹 삭제**를 선택합니다.
4. **리소스 그룹 삭제** 페이지의 **리소스 그룹 이름 입력**에서 삭제를 확인하고 **myVNetNSGRG**를 입력한 다음 **삭제**를 선택합니다.
5. **Delete**를 다시 선택합니다.