

# 가상 네트워크(VNet) 만들기

주신영 bit1010@live.com

이번 실습은 MS의 실습 자료를 참고하였습니다.

빠른 시작: Azure 포털을 사용하여 가상 네트워크 만들기

Azure Bastion 사용 유무를 선택하도록 수정하였습니다.

Azure Bastion을 사용하지 않을 경우는 공용IP와 인바운드(3389)를 추가하고 원격 데스크톱을 이용해서 연결합니다.



일반적으로 **베스천(Bastion)** 또는 **점프박스(Jumpbox)**는 관리자를 위한 보안 요소로 적용합니다.

22,3389 포트 등의 서버 관리 포트는 외부(인터넷)에 바로 노출되지 않고 베스천을 통해 연결합니다.

일종의 프록시와 같으며 관리자가 작업한 내역을 로그로 남겨 추적이 가능하고 베스천으로 연결되는 물리적인 네트워크 또한 사내망이나 VPN등으로 제한합니다.

일반 서비스(http 등)를 위해 사용하지 않습니다.

Azure Bastion은 VNet 생성후에도 Bastion 메뉴에서 추가 가능합니다.

Bastion 삭제는 VNet메뉴가 아닌 Bastion에서 삭제를 하면 됩니다.

지역은 계정에 제한이 없다면 Korea Central을 선택합니다.



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

Windows 가상 머신(VM) 만들기 실습을 다시 진행해서 가상 네트워크가 자동으로 생성되고 가상머신에 적용된 사항을 먼저 확인합니다.

## 가상 네트워크 만들기

이전 실습에서 가상머신 생성 시 VNet은 기본 설정으로 생성됐습니다. 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 *myVNetRG*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 주소를 선택합니다.

5. IP 주소 탭의 IPv4 주소 공간에서 10.0.0.0/16을 입력합니다.

\* 주소공간이 변경되면 기본 설정된 서브넷이 삭제됩니다.

6. 서브넷 추가를 선택합니다.

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

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

The screenshot shows the 'Create virtual network' page in the Azure portal. The 'IP Addresses' tab is selected and highlighted with a red box. Below the tab, the 'IPv4 address space' is set to '10.0.0.0/16'. A table lists the subnets, with a red box around the '+ Add subnet' button. The 'Add subnet' dialog is open on the right, showing the 'Subnet name' as 'default' and the 'Subnet address range' as '10.0.0.0/24'. The dialog also includes sections for 'NAT GATEWAY' and 'SERVICE ENDPOINTS'.

Home > Virtual networks > Create virtual network ...

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation.

IPv4 address space

10.0.0.0/16

☐ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained within the virtual network's address space.

**+ Add subnet** Remove subnet

<input type="checkbox"/> Subnet name	Subnet address range
<input type="checkbox"/> default	10.0.0.0/24

**i** A NAT gateway is recommended for outbound internet access from subnets. Edit the virtual network to add a NAT gateway.

Review + create < Previous Next : Security Add Cancel

**Add subnet**

Subnet name \* default

Subnet address range \* ⓘ 10.0.0.0/24 (0 Addresses)

**NAT GATEWAY**

Simplify connectivity to the internet using a network address translation gateway. Outbound connectivity is possible without a load balancer or public IP addresses attached to your virtual machines. [Learn more](#)

NAT gateway None

**SERVICE ENDPOINTS**

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ 0 selected

8. Azure Bastion 사용 유무를 선택합니다.

#### ▼ Azure Bastion 설정

- a. 페이지 하단에서 **다음: 보안**을 선택합니다.
- b. 보안 탭의 **BastionHost** 옆에 있는 **사용**을 선택합니다.
- c. 다음 정보를 입력합니다.
  - 베스천 이름: bastion
  - AzureBastionSubnet 주소 공간: 10.0.1.0/26  
Azure는 AzureBastionSubnet 서브넷을 자동으로 만듭니다.
  - 공용 IP 주소: 새로 만들기를 선택한 다음 이름 아래에 *bastionPip*을 입력하고 **확인**을 선택합니다.

**\* 베스천 서브넷이 화면에 안나올 수도 있음. 자동으로 생성되므로 넘어가면 됨.**

Azure Bastion을 설정하면 생성하는데 시간이 좀 더 필요합니다.

9. 화면 아래쪽에서 **검토 + 만들기** 를 선택하고 유효성 검사가 통과되면 **만들기**를 선택합니다.

## 가상 머신 만들기

가상 네트워크에 VM1 및 VM2라는 두 개의 VM을 만듭니다.

1. 포털에서 **가상 머신**을 검색하고 선택합니다.
2. **가상 머신** 페이지에서 **만들기**를 선택하고 **Azure 가상 머신**을 선택합니다.
3. **가상 머신 만들기** 화면의 **기본 사항** 탭에서 다음 값을 입력하거나 선택합니다.
  - **리소스 그룹:** *myVNetRG*를 선택합니다.
  - **가상 머신 이름:** *VM1*을 입력합니다.
  - **지역:** 가상 네트워크와 동일한 지역을 선택합니다.
  - **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:** **RDP(3389)**를 선택합니다.(기본으로 선택되어 있음)

## 가상 머신 만들기 ...

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 myVNetRG ▼  
[새로 만들기](#)

**인스턴스 정보**

가상 머신 이름 \* ① VM1 ✓

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**) **VM1-ip**

### ▼ Azure Bastion 설정

**공용 IP :** 없음

**NIC 네트워크 보안 그룹 :** 없음?

**공용 인바운드 포트 :** 없음

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, 인바운드 및 아웃바운드 연결을 제어하거나 기존 부하 분산 솔루션 뒤에 배치할 수 있습니다. [자세한 정보](#)

### 네트워크 인터페이스

가상 머신을 만들면 네트워크 인터페이스가 만들어집니다.

가상 네트워크 \* ⓘ

VNet  
[새로 만들기](#)

서브넷 \* ⓘ

default(10.0.0.0/24)  
[서브넷 구성 관리](#)

공용 IP ⓘ

(새로 만드는 중) VM1-ip  
[새로 만들기](#)

NIC 네트워크 보안 그룹 ⓘ

☐ 없음  
☒ 기본  
☐ 고급

공용 인바운드 포트 \* ⓘ

☐ 없음  
☒ 선택한 포트 허용

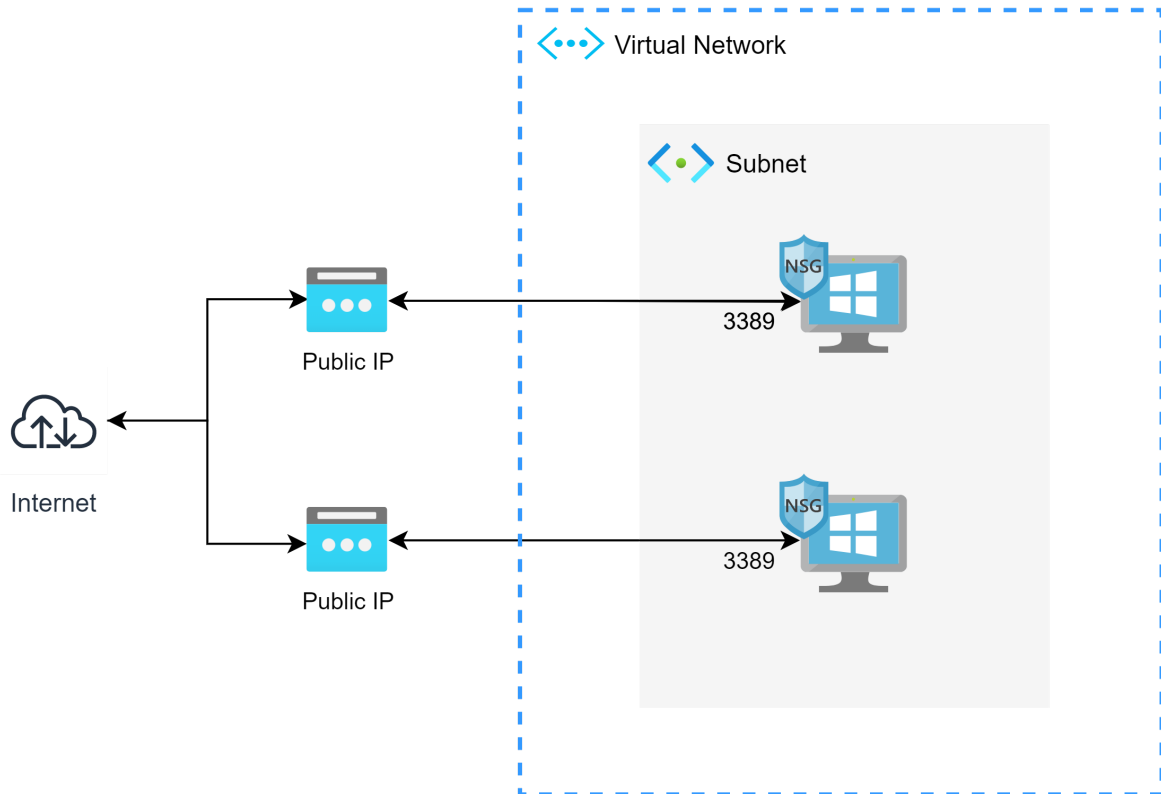
인바운드 포트 선택 \*

RDP (3389)

⚠ 이렇게 하면 모든 IP 주소가 가상 머신에 액세스할 수 있습니다. 이는 테스트용으로만 권장됩니다. [네트워킹] 탭의 [고급] 컨트롤을 사용하여 인바운드 트래픽을 알려진 IP 주소로 제한하는 규칙을 만듭니다.

- 다른 설정을 적용하고 **검토 + 만들기**를 선택합니다. 설정을 검토한 다음, **만들기**를 선택합니다.
- VM 만들기가 완료되면 **다른 VM 만들기**를 선택하여 **두 번째 VM**을 만들 수 있습니다. 모든 동일한 설정을 사용하여 **VM2**의 이름으로 생성합니다.

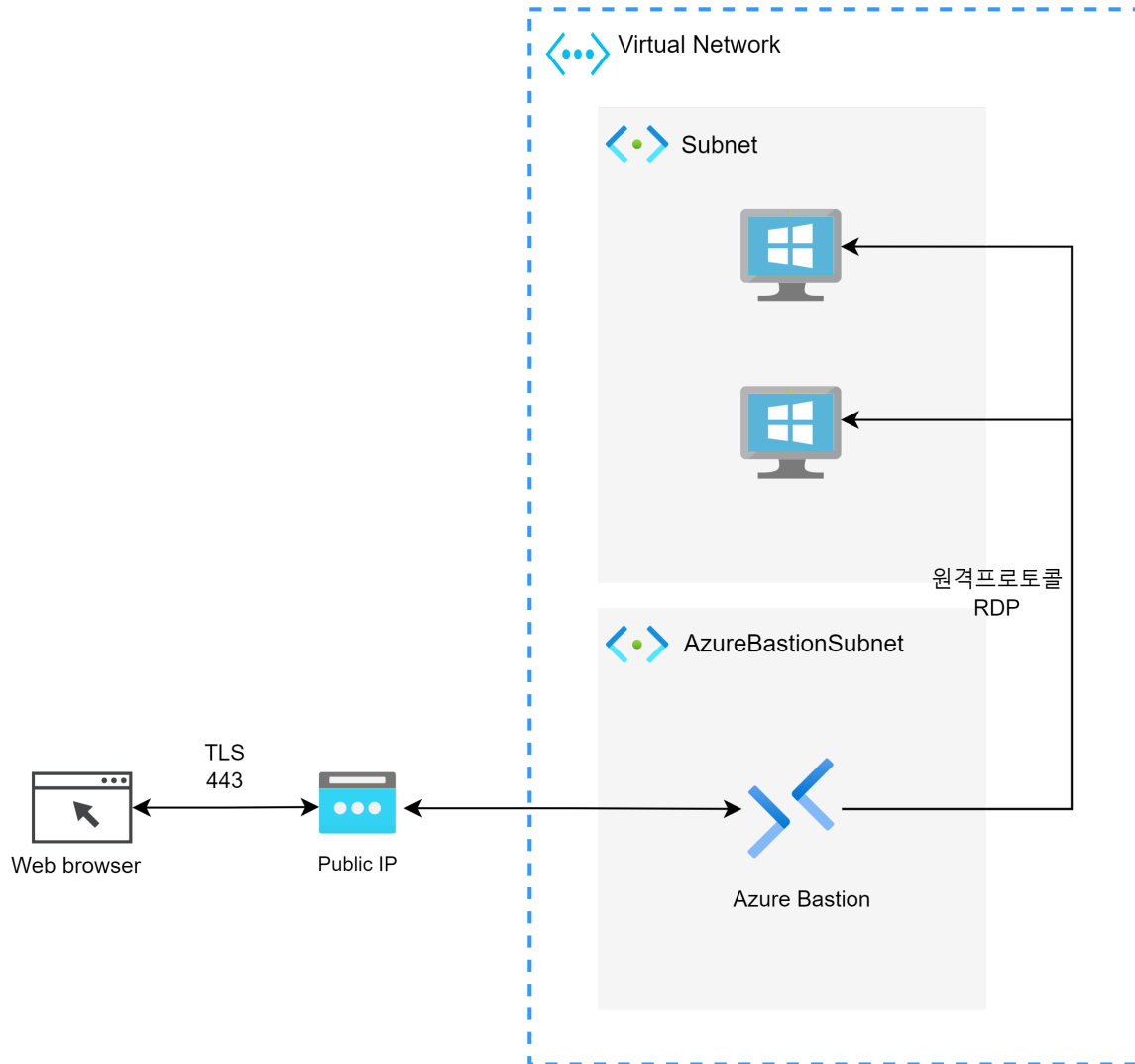
## 리소스 그룹에 생성된 리소스 확인



## Azure Bastion 사용 구성

웹 브라우저에서 Azure Bastion으로 웹 프로토콜(HTTPS)로 연결되며 Azure Bastion과 가상머신은 가상 네트워크 내에서 연결됩니다. 네트워크 보안 그룹은 사용하지 않지만 외부에서 가상머신으로 연결하는 포트가 필요하다면 네트워크 보안 그룹이 필요합니다.





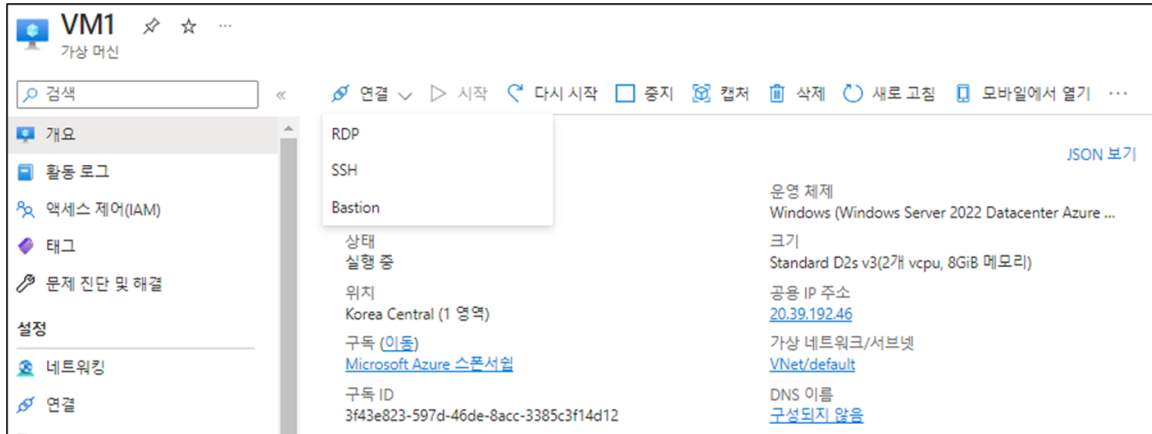
## VM에 연결

1. 포털에서 **가상 머신**을 검색하고 선택합니다.
2. **가상 머신** 페이지에서 **VM1**을 선택합니다.
3. **VM1** 페이지의 맨 위에서 **연결** 옆에 있는 드롭다운 화살표를 선택한 다음 **RDP 파일**을 다운로드 받은 파일로 실행하거나 **원격데스크탑(RDP)**를 로컬PC에서 실행해서 공용 IP 주소로 접속합니다.

### ▼ Azure Bastion 설정

연결에서 **Bastion**을 선택합니다.

**Bastion** 페이지에서 VM에 대해 만든 사용자 이름 및 암호를 입력한 다음 **연결**을 선택합니다.



4. VM에 입력한 사용자 이름 및 암호를 입력한 다음 **연결**을 선택합니다.

5. **VM2**도 동일하게 연결합니다.

## VM 간 통신

1. VM1의 데스크톱에서 PowerShell을 엽니다.

2. `ping VM2`를 입력합니다. 다음 메시지와 유사한 회신이 표시됩니다.

```
PS C:\Users\VM1> ping VM2
```

```
Pinging VM2.ovvzzdcazhbu5iczfvonhg2zrb.bx.internal.cloud
app.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% los
s),
```



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. VM2도 동일하게 연결하여 PowerShell에서 `ping VM1` 를 입력합니다  
이번에는 VM1의 방화벽을 통해 ICMP를 허용했기 때문에 다음 메시지와 유사한 성공 회신이 표시됩니다.

반대로 VM2에서도 ICMP를 허용하도록 설정하고 VM1에서 `ping VM2` 을 입력합니다.

```
PS C:\Users\VM2> ping VM1
```

```
Pinging VM1.e5p2dibbrqtejhq04lgrusvd4g.bx.internal.cloud  
app.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. VM1과 2 연결한 원격 데스크탑 또는 Bastion페이지를 닫습니다.

## 리소스 정리