

Lab12. 가상 네트워크를 통해 2개의 VM 연결하기

1. 목적

이번 실습에서는 가상 네트워크를 생성하고 두 개의 가상 머신을 해당 가상 네트워크에 배포한 다음, 가상 네트워크 내에서 한 개의 가상 머신이 다른 가상 머신을 ping 하도록 구성한다.

2. 사전 준비물

- Azure 체험 계정

3. 가상 네트워크 생성하기

A. **Azure Portal**에 로그인한다. 전역 검색 창에서 **가상 네트워크**를 검색하여 선택한다.



B. **[가상 네트워크]** 페이지로 들어왔다. **[+만들기]**를 클릭한다.



C. **[가상 네트워크 만들기]** 블레이드의 **[기본 사항]** 탭에서 다음의 각 값을 설정하고, 나머지 값들은 그대로 기본값을 사용하기로 한다. 모두 설정한 후 **[다음:IP 주소 >]**를 클릭한다.

- ① 구독 : 현재 계정의 구독
- ② 리소스 그룹 : [새로 만들기] > myRGVNet

③ 이름 : vnet1

④ 지역 : (Asiz Pacific) 한국 중부

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 * ① MSDN 플랫폼 구독

리소스 그룹 * ① (신규) myRGVNet
[새로 만들기](#)

인스턴스 정보

이름 * vnet1

지역 * (Asia Pacific) 한국 중부

검토 + 만들기 < 이전 다음: IP 주소 > 자동화에 대한 템플릿 다운로드

D. [IP 주소] 탭에서 다음의 각 값을 설정한다. 그리고 [검토 + 만들기] 버튼을 클릭한다.

① IPv4 주소 공간 : 10.1.0.0/16

② 서브넷 : default (10.1.0.0/24)

가상 네트워크 만들기 ...

기본 사항 IP 주소 보안 태그 검토 + 만들기

CIDR 표기법으로 된 하나 이상의 주소 접두사로 지정된 가상 네트워크의 주소 공간입니다(예: 192.168.1.0/24).

IPv4 주소 공간

10.1.0.0/16 10.1.0.0 - 10.1.255.255(65536개 주소)

☐ IPv6 주소 공간 추가 ①

서브넷의 주소 범위가 CIDR 표기법(예: 192.168.1.0/24)으로 되어 있습니다. 이 주소 범위는 가상 네트워크의 주소 공간에 포함되어야 합니다.

+ 서브넷 추가 - 서브넷 제거

서브넷 이름	서브넷 주소 범위	NAT 게이트웨이
<input type="checkbox"/> default	10.1.0.0/24	-

검토 + 만들기 < 이전 다음: 보안 > 자동화에 대한 템플릿 다운로드

E. [유효성 검사 통과] 후 [만들기] 버튼을 클릭한다.

가상 네트워크 만들기

유효성 검사 통과

기본 사항IP 주소보안태그검토 + 만들기

기본 사항

구독

리소스 그룹

이름

지역

MSDN 플랫폼 구독

(새로 만드는 중) myRGVNet

vnet1

한국 중부

IP 주소

주소 공간

서브넷

10.1.0.0/16

default(10.1.0.0/24)

태그

만들기

< 이전

다음 >

자동화에 대한 템플릿 다운로드

F. [배포가 완료됨]을 확인하면, [리소스로 이동] 버튼을 클릭한다.

배포가 완료됨

배포 이름: Microsoft.VirtualNetwork-20210718141137

시작 시간: 2021. 7. 18. 오후 2:19:51

구독: MSDN 플랫폼 구독

상관 관계 ID: 2e6e085e-1005-4601-b7f7-ad05f6ff31ee

리소스 그룹: myRGVNet

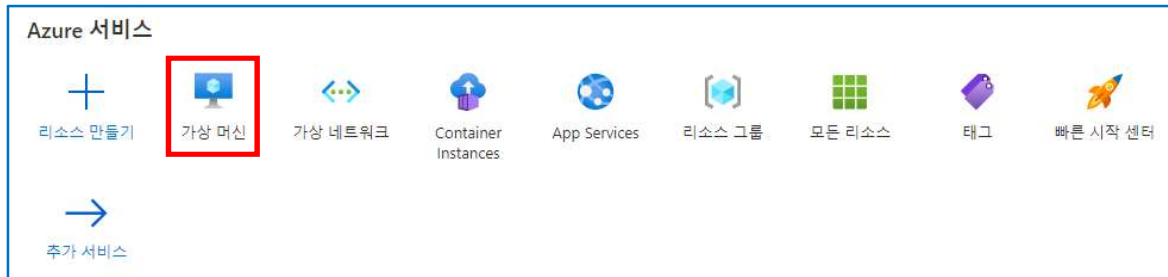
배포 정보 (다운로드)

다음 단계

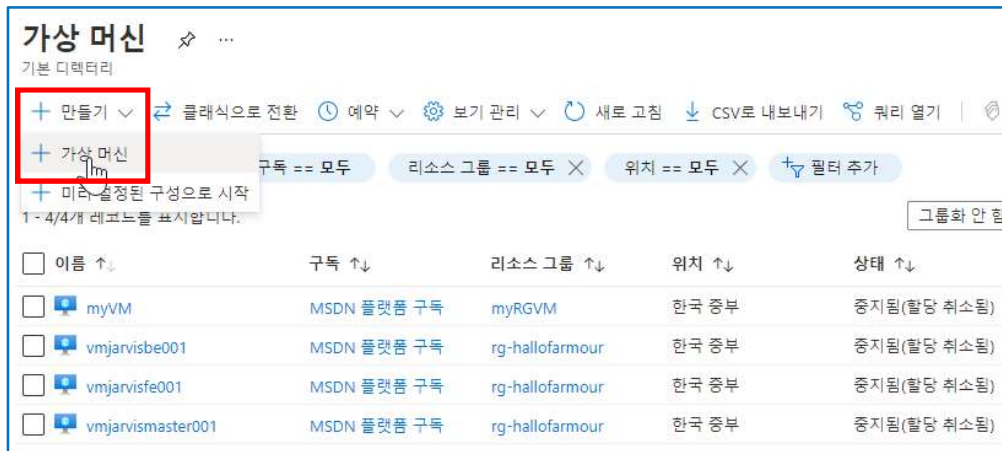
리소스로 이동

4. 가상 머신 2개 생성하기

A. **Azure Portal** 페이지에서 **[Azure 서비스]** 섹션의 **[가상 머신]**을 클릭한다.



B. **[가상 머신]** 블레이드에서 **[+만들기]** > **[가상 머신]**를 클릭한다.



C. **[가상 머신 만들기]** 블레이드의 **[기본 사항]** 탭에서 다음의 각 값을 설정하고, 나머지는 기본값 그대로 사용하기로 한다.

- ① 구독 : 현재 계정의 구독
- ② 리소스 그룹 : myRGVNet
- ③ 가상 머신 이름 : vm1
- ④ 지역 : (Asia Pacific) 한국 중부
- ⑤ 이미지 : Windows Server 2019 Datacenter – Gen1

가상 머신 만들기

기본 사항 디스크 네트워킹 관리 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 MSDN 플랫폼 구독

리소스 그룹 * ① myRGVNet
[새로 만들기](#)

인스턴스 정보

가상 머신 이름 * ① vm1 ✓

지역 * ① (Asia Pacific) 한국 중부 ✓

가용성 옵션 ① 인프라 중복이 필요하지 않습니다. ✓

이미지 * ① Windows Server 2019 Datacenter - Gen1 ✓
[모든 이미지 보기](#)

D. 계속해서 다음의 각 값을 설정한다.

- ① 사용자 이름 : azureuser
- ② 암호 / 암호 확인 : P@\$W0rd1234
- ③ 공용 인바운드 포트 : 선택한 포트 허용
- ④ 인바운드 포트 선택 : RDP(3389)

관리자 계정

사용자 이름 * ① azureuser ✓

암호 * ① ✓

암호 확인 * ① ✓

인바운드 포트 규칙
공용 인터넷에서 액세스할 수 있는 가상 머신 네트워크 포트를 선택하세요. [네트워킹] 탭에서 더 제한되거나 세분화된 네트워크 액세스를 지정할 수 있습니다.

공용 인바운드 포트 * ① ☐ 없음 ☒ 선택한 포트 허용

인바운드 포트 선택 * RDP (3389) ✓

E. [네트워킹] 탭으로 이동하여 지금 생성하려는 가상 머신의 가상 네트워크가 **vnet1**인지 확인한다. 나머지 값들을 기본값 그대로 놓고, [검토 + 만들기] 버튼을 클릭한다.

가상 머신 만들기 ...

기본 사항 디스크 **네트워킹** 관리 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 vnet1 새로 만들기

서브넷 * ① default(10.1.0.0/24) 서브넷 구성 관리

공용 IP ① {새로 만드는 중} vm1-ip 새로 만들기

NIC 네트워크 보안 그룹 ① ☐ 없음 ☒ 기본 ☐ 고급

검토 + 만들기 < 이전 다음: 관리 >

F. [유효성 검사 통과]를 확인 후, [만들기]를 클릭한다.

가상 머신 만들기 ...

유효성 검사 통과

기본 사항 디스크 네트워킹 관리 고급 태그 **검토 + 만들기**

제품 정보

표준 DS1 v2 구독 크레딧 적용 ①

Microsoft **92.7836KRW/시간**

[사용 약관](#) | [개인 정보 취급 방침](#) [다른 VM 크기에 대한 가격 책정](#)

사용 약관

"만들기"을(를) 클릭함으로써 본인은 (a) 위의 해당 Marketplace 제품과 관련된 약관 및 개인정보처리방침에 동의하고, (b) Microsoft가 현재 결제 방법으로 제품과 관련된 요금을 내 Azure 구독과 동일한 대금 청구 주기로 청구하도록 권한을 부여하는 데 동의합니다. 또한 (c) Microsoft가 지원, 청구 및 기타 거래 목적으로 내 연락처 정보, 트랜잭션 정보 및 사용량 정보를 제품 공급자와 공유할 수 있다는 데 동의합니다. Microsoft는 타사 제품에 대한 권리를 제공하지 않습니다. 자세한 내용은 Azure Marketplace 사용 약관을 참조하세요.

만들기 < 이전 다음 > [자동화에 대한 템플릿 다운로드](#)

G. 두번째 가상 머신을 생성하기 위해, 위의 A ~ F까지의 과정을 한 번 수행하되, 다음의 각 값들의 설정만 유의하여 생성한다.

- ① 리소스 그룹 : myRGVNet
- ② 가상 머신 이름 : vm2
- ③ 가상 네트워크 : vnet1
- ④ 공용 IP : vm2-ip

가상 머신 만들기 ...

⚠ 기본 옵션을 변경하면 선택한 내용이 다시 설정될 수 있습니다. 가상 머신을 만들기 전에 모든 옵션을 검토하세요.

기본 사항 디스크 네트워킹 관리 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

MSDN 플랫폼 구독

리소스 그룹 * ①

myRGVNet

[새로 만들기](#)

인스턴스 정보

가상 머신 이름 * ①

vm2

지역 * ①

(Asia Pacific) 한국 중부

가용성 옵션 ①

인프라 중복이 필요하지 않습니다.

이미지 * ①

Windows Server 2019 Datacenter - Gen1

크기 * ①

Standard_DS1_v2 - 1 vcpu, 3.5 GiB 메모리 (₩67,732/월)

[모든 크기 보기](#)

관리자 계정

사용자 이름 * ①

azureuser

암호 * ①

.....

암호 확인 * ①

.....

인바운드 포트 규칙

공용 인터넷에서 액세스할 수 있는 가상 머신 네트워크 포트를 선택하세요. [네트워킹] 탭에서 더 제한되거나 세분화된 네트워크 액세스를 지정할 수 있습니다.

공용 인바운드 포트 * ①

- ☐ 없음
☒ 선택한 포트 허용

인바운드 포트 선택 *

RDP (3389)

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 * ①

vnet1

[새로 만들기](#)

서브넷 * ①

default(10.1.0.0/24)

[서브넷 구성 관리](#)

공용 IP ①

(새로 만드는 중) vm2-ip

[새로 만들기](#)

NIC 네트워크 보안 그룹 ①

- ☐ 없음
☒ 기본
☐ 고급

- H. 첫번째 가상 머신 생성과 마찬가지로 [검토 + 만들기]를 클릭하고 [유효성 검사 통과] 확인 후, [만들기]를 클릭한다.

가상 머신 만들기 ...

유효성 검사 통과

기본 사항 디스크 네트워킹 관리 고급 태그 검토 + 만들기

제품 정보

표준 DS1 v2 구독 크레딧 적용 ①
Microsoft 92.7836KRW/시간
사용 약관 | 개인 정보 취급 방침 다른 VM 크기에 대한 가격 책정

사용 약관

"만들기"를 클릭함으로써, 본인은 (a) 위의 해당 Marketplace 제품과 관련된 약관 및 개인정보처리방침에 동의하고, (b) Microsoft가 현재 결제 방법으로 제품과 관련된 요금을 내 Azure 구독과 동일한 대금 청구 주기로 청구하도록 권한을 부여하는 데 동의합니다. 또한 (c) Microsoft가 지원, 청구 및 기타 거래 목적으로 내 연락처 정보, 트랜잭션 정보 및 사용량 정보를 제품 공급자와 공유할 수 있다는 데 동의합니다. Microsoft는 타사 제품에 대한 권리를 제공하지 않습니다. 자세한 내용은 [Azure Marketplace 사용 약관](#)을 참조하세요.

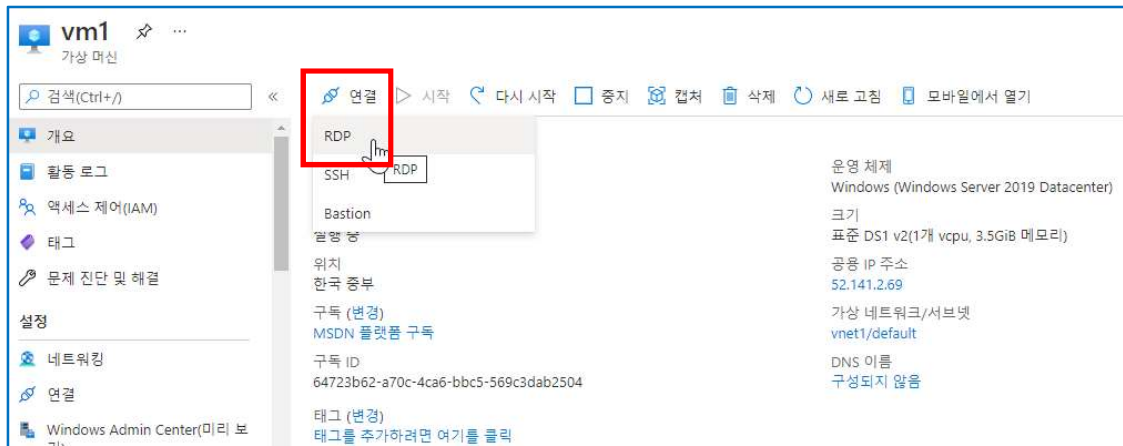
만들기

< 이전 다음 > 자동화에 대한 템플릿 다운로드

- I. 두 개의 가상 머신이 모두 생성 및 배포될 때까지 기다린다.

5. 연결 테스트

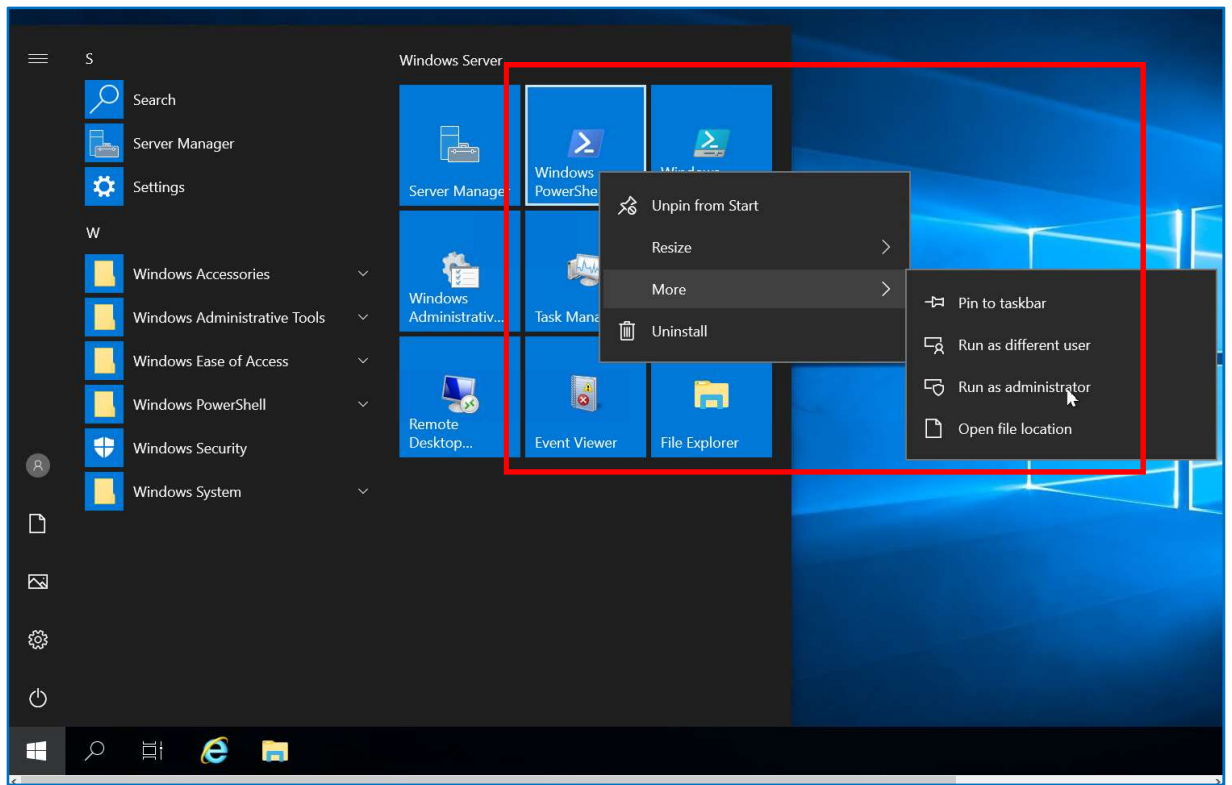
- A. 먼저 생성한 가상 머신 vm1을 RDP를 통해 연결한다. 해당 가상 머신 **[개요]** 블레이드에서 명령바의 **[연결]** > **[RDP]**를 선택한다.



- B. **[RDP 파일 다운로드]** 하여 RDP를 통해 **vm1**과 연결한다. 유저는 **azureuser**이고 암호는 **P@\$W0rd1234**이다.



- C. 해당 가상 머신에서 **[Windows PowerShell]**을 관리자 권한으로 었다.

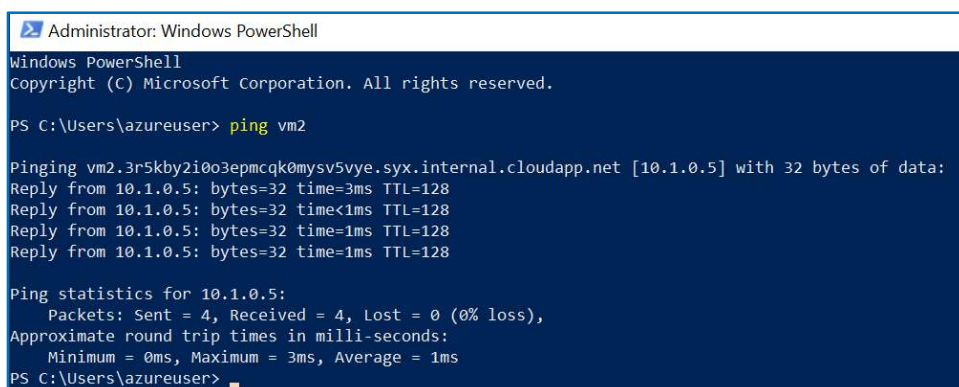


D. Azure Portal로 돌아와서 **vm2** 가상 머신의 [상태]가 **실행 중** 임을 확인한다.

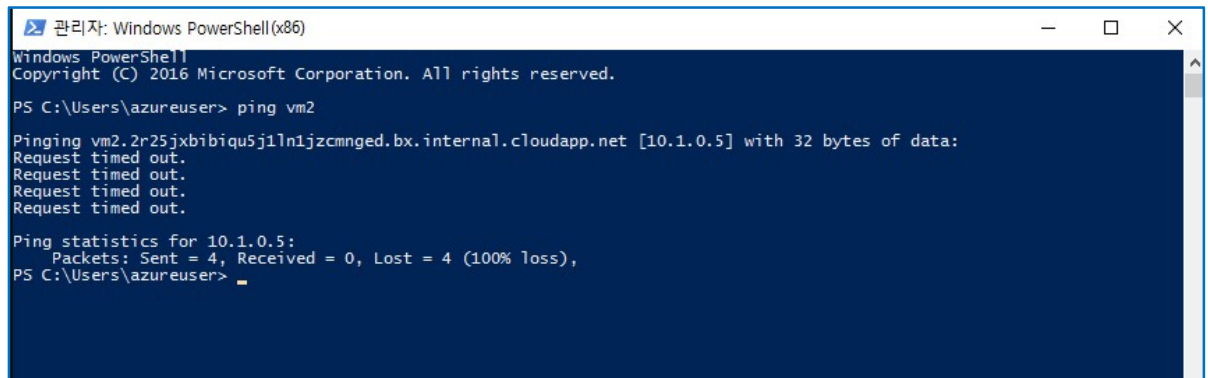


E. 방금 연결한 가상 머신 **vm1**에서 **vm2**에 **ping** 테스트를 시행한다.

ping vm2



- F. 혹은 다음 그림과 같이 **ping** 테스트에 실패할 수 있다. 요청 시간이 초과되었다는 내용의 오류 메시지이다. **ping**은 **ICMP(인터넷 제어 메시지 프로토콜)**을 사용하기 때문에 **ping**이 실패할 수 있다. **ping**이 실패한다는 것은 해당 가상 머신의 **Windows 방화벽**이 허용하지 않았기 때문이다.



```
관리자: Windows PowerShell(x86)
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

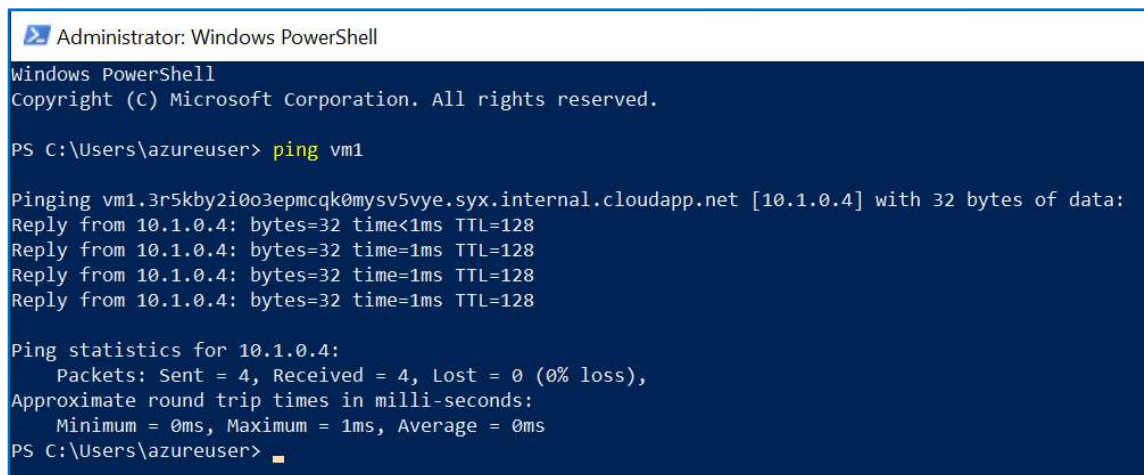
PS C:\Users\azureuser> ping vm2

Pinging vm2.2r25jxbibiqu5j1ln1jzcmnged.bx.internal.cloudapp.net [10.1.0.5] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\azureuser>
```

- G. 두번째 가상 머신도 RDP 3389 포트를 통해 연결한다. 두번째 가상 머신인 **vm2**에서도 **vm1**을 향해 **ping** 테스트를 수행한다.

ping vm1



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\azureuser> ping vm1

Pinging vm1.3r5kby2i0o3epmcqk0mysv5vye.syx.internal.cloudapp.net [10.1.0.4] with 32 bytes of data:
Reply from 10.1.0.4: bytes=32 time<1ms TTL=128
Reply from 10.1.0.4: bytes=32 time=1ms TTL=128
Reply from 10.1.0.4: bytes=32 time=1ms TTL=128
Reply from 10.1.0.4: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\azureuser>
```

- H. 역시 **vm2**에서도 **vm1**에 **ping** 테스트를 성공적으로 수행했다.
- I. 만일 **ping** 테스트를 성공적으로 수행하지 못했을 때에는 다음과 같은 작업을 수행한다. 먼저 **PowerShell 명령 프롬프트**에서 **ICMP**를 허용한다. 이 명령은 **Windows 방화벽**을 통한 **ICMP 인바운드 연결**을 허용하는 명령이다.

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

```
Administrator: Windows PowerShell
PS C:\Users\azureuser> New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4

Name                : {59682308-34a5-4758-88d4-a97015d6c880}
DisplayName          : Allow ICMPv4-In
Description          :
DisplayGroup         :
Group                :
Enabled              : True
Profile              : Any
Platform             : {}
Direction            : Inbound
Action               : Allow
EdgeTraversalPolicy  : Block
LooseSourceMapping   : False
LocalOnlyMapping     : False
Owner                :
PrimaryStatus        : OK
Status               : The rule was parsed successfully from the store. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource    : PersistentStore
PolicyStoreSourceType : Local

PS C:\Users\azureuser> █
```

- J. 위의 명령을 두개의 가상 머신 모두에서 수행한 후, 다시 서로 **ping 테스트**를 수행한다.