

Lab4. Windows 10 VM 만들고 연결하기

1. 목적

- Microsoft Azure에 가상 머신을 설치하고, 가상 머신에서 WSL2를 통해 Ubuntu Server를 가상화로 설치해서 Ubuntu Server에 연결한다.

2. 사전 준비물

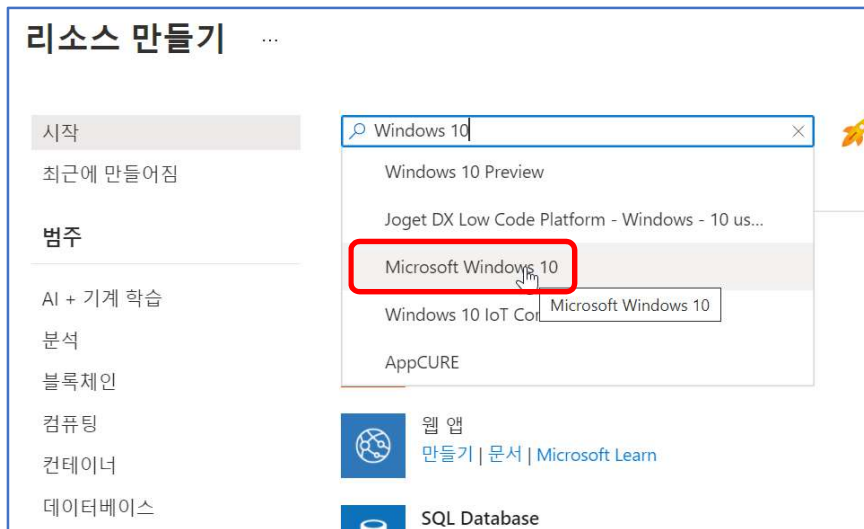
- Microsoft Azure 체험 계정
- rg-hallofarmour 리소스 그룹
- vnet-hallofarmour-krcentral-001 가상 네트워크
- snet-jarvis 서버넷

3. 가상 머신 만들기

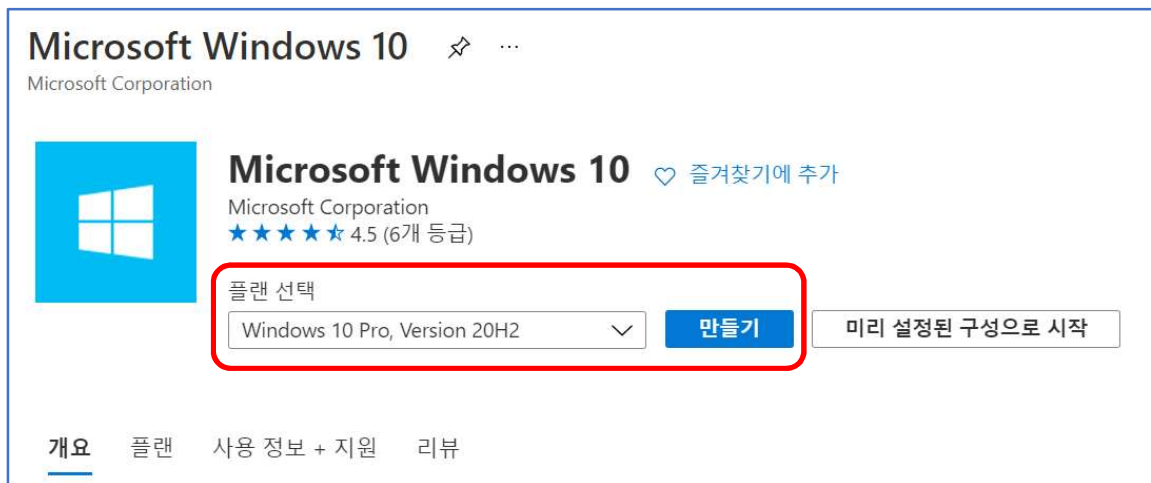
- A. Microsoft Azure Portal 페이지(<https://portal.azure.com>)로 이동하여 로그인한다. 페이지 상단의 [Azure 서비스] 섹션에서 [리소스 만들기] 버튼을 클릭한다 .



- B. [리소스 만들기] 블레이드의 검색 창에 **Windows 10**을 입력한 다음 **Microsoft Windows 10**을 선택한다.



- C. **[Microsoft Windows 10]** 블레이드에서 **[플랜 선택]**의 목록 중 기본 최신 플랜을 선택하고 **[만들기]**를 클릭한다 .



- D. **[가상 머신 만들기]** 블레이드에서 다음과 같이 **[기본 사항]** 탭의 각각의 값들을 입력한다.

- ① 구독 : 현재 계정의 구독
- ② 리소스 그룹 : rg-hallofarmour
- ③ 가상 머신 이름 : vmjarvismaster001
- ④ 지역 : (Asia Pacific) 한국 중부
- ⑤ 가용성 옵션 : 인프라 중복이 필요하지 않습니다.
- ⑥ 이미지 : Windows 10 Pro, Version 20H2 – Gen1
- ⑦ Azure 스폿 인스턴스 : No Check
- ⑧ 크기 : Standard_DS2_v2 – 2 vcpu, 7 GiB 메모리 (₩135,464/월)

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

(새로운) 리소스 그룹

[새로 만들기](#)

- E. 계속해서 관리자 계정 정보와 인바운드 포트 규칙, 라이선싱 정보를 다음과 같이 각 각의 값을 입력한다음, [다음: 디스크] 버튼을 클릭한다.

- ① 사용자 이름 : tony
- ② 암호 : P@\$W0rd1234
- ③ 암호 확인 : P@\$W0rd1234
- ④ 공용 인바운드 포트 : 선택한 포트 허용
- ⑤ 인바운드 포트 선택 : RDP (3389)
- ⑥ 라이선싱 : 체크

관리자 계정

사용자 이름 * ①

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)

- F. [디스크]탭에서 [OS 디스크 유형]은 표준 SSD(로컬 중복 스토리지)를 선택하고 나머지 항목들은 기본값 그대로 둔 다음, [다음:네트워킹] 버튼을 클릭한다.

기본 사항 **디스크** 네트워킹 관리 고급 태그 검토 + 만들기

Azure VM에 하나의 운영 체제 디스크와 단기 저장을 위한 임시 디스크가 있습니다. 추가 데이터 디스크를 연결할 수 있습니다. VM의 크기에 따라 사용 가능한 스토리지 유형 및 허용된 데이터 디스크 수가 결정됩니다. [자세한 정보](#)

디스크 옵션

OS 디스크 유형 * ① 표준 SSD(로컬 중복 스토리지) ▼
선택한 VM 크기는 프리미엄 디스크를 지원하지 않습니다. IOPS가 높은 워크로드의 경우 프리미엄 SSD를 사용하는 것이 좋습니다. 프리미엄 SSD 디스크를 사용하는 가상 머신은 99.9%의 연결 SLA를 제공합니다.

SSE 암호화 유형 * (기본값) 플랫폼 관리형 키로 미사용 데이터 암호화 ▼

Ultra Disk 호환성 사용 ① ☐
koreacentral의 선택한 VM 크기 Standard_DS2_v2에 대해서는 Ultra Disk가 지원되지 않습니다.

데이터 디스크

검토 + 만들기 < 이전 다음: 네트워킹 >

- G. [네트워킹]를 탭에서 다음의 각 값을 설정하고 나머지값은 기본값 그대로 둔 뒤, [다음:관리] 버튼을 클릭한다.

① 가상 네트워크 : vnet-hallofarmour-krcentral-001

② 서버넷 : snet-javis(172.16.1.0/24)

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, 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 vnet-hallofarmour-krcentral-001 ▼
[새로 만들기](#)

서버넷 * ① snet-javis(172.16.1.0/24) ▼
[서버넷 구성 관리](#)

공용 IP ① (새로 만드는 중) vmjarvismaster001-ip ▼
[새로 만들기](#)

NIC 네트워크 보안 그룹 ① ☐ 없음 ☐ 기본

검토 + 만들기 < 이전 다음: 관리 >

- H. [관리] 탭에서 [부트 진단]을 [사용 안함]을 선택하고, 나머지는 기본값 그대로 둔 뒤, [다음:고급]을 클릭한다.

기본 사항 디스크 네트워크 **관리** 고급 태그 검토 + 만들기

VM에 대한 모니터링 및 관리 옵션을 구성합니다.

Azure Security Center

Azure Security Center는 하이브리드 클라우드 워크로드에서 통합 보안 관리 및 지능형 위협 방지 기능을 제공합니다.
[자세한 정보](#)

✓ 구독은 Azure Security Center 기본 플랜으로 보호됩니다.

모니터링

부트 진단 ⓘ

☐ 관리형 스토리지 계정으로 사용하도록 설정(권장)

☐ 사용자 지정 스토리지 계정으로 사용하도록 설정

☒ 사용 안 함

OS 게스트 진단 사용 ⓘ ☐

검토 + 만들기 < 이전 다음: 고급 >

- I. [고급] 탭에서 맬웨어 방지를 위해 [확장] 섹션에서 [설치할 확장 선택]을 클릭한다.

기본 사항 디스크 네트워크 관리 **고급** 태그 검토 + 만들기

가상 머신 확장 또는 Cloud-Init를 통해 추가 구성, 에이전트, 스크립트 또는 애플리케이션을 추가합니다.







확장

확장은 배포 후 구성 및 자동화를 제공합니다.

확장 ⓘ **설치할 확장 선택**

- J. [새 리소스] 블레이드가 나타났다. 여기서 목록 중에 [Microsoft Antimalware]를 선택한다.

새 리소스 ✨ ...

	Dynatrace OneAgent Dynatrace
	ESET File Security ESET
	HPE Security Fortify Application Defender HPE Security Fortify
	Kaspersky Hybrid Cloud Security Agent Kaspersky Lab
	Microsoft Antimalware Microsoft Corp.
	NVIDIA GPU Driver Extension Microsoft Corp.

- K. [Microsoft Antimalware] 블레이드에서 [만들기] 버튼을 클릭한다.

Microsoft Antimalware

Microsoft Corp.

Microsoft Antimalware for Azure Virtual Machines is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your system. The solution can be enabled and configured from the Azure Portal, Service Management REST API, and Microsoft Azure PowerShell SDK cmdlets.

To **enable** antimalware with the **default configuration**, click **Create** on the Add Extension blade without inputting any configuration setting values.

To **enable** antimalware with a **custom configuration**, input the supported values for the configuration settings provided on the **Add Extension** blade and click **Create**. Please refer to the **tooltips** provided with each configuration setting on the Add Extension blade to see the supported configuration values.

To **enable antimalware event collection** for a virtual machine, click any part of the **Monitoring lens** in the virtual machine blade, click **Diagnostics** command on Metric blade, select **Status ON** and check **Windows Event system logs**. The antimalware events are collected from the Windows Event system logs to your storage account. You can configure the storage account for your virtual machine to collect the antimalware events by selecting the appropriate storage account.

Legal Terms

By clicking the Create button, I acknowledge that I am getting this software from Microsoft Corp. and that the [legal terms](#) of Microsoft Corp. apply to it. Microsoft does not provide rights for third-party software. Also see the [privacy statement](#) from Microsoft Corp..

게시자
Microsoft Corp.

만들기

- L. [확장 설치] 블레이드에서 기본값 그대로 놓고, [확인] 버튼을 클릭한다.

확장 설치

Excluded files and locations ⓘ

Excluded file extensions ⓘ

Excluded processes ⓘ

Real-time protection ⓘ
Enable Disable

Run a scheduled scan ⓘ
Enable Disable

Scan type ⓘ
Quick Full

Scan day ⓘ

확인

- M. 다시 [가상 머신 만들기] 블레이드로 돌아왔다. [확장]에서 방금 생성한 **Microsoft Antimalware**를 확인하고 [검토 + 만들기]를 클릭한다.

가상 머신 만들기 ...

가상 머신 확장 또는 Cloud-Init를 통해 추가 구성, 에이전트, 스크립트 또는 애플리케이션을 추가합니다.

확장

확장은 배포 후 구성 및 자동화를 제공합니다.

확장 ⓘ

Microsoft Antimalware
Microsoft Corp.

✎ 🗑

[설치할 확장 선택](#)

사용자 지정 데이터

가상 머신이 프로비저닝되는 동안 스크립트, 구성 파일 또는 기타 데이터를 가상 머신으로 전달합니다. 데이터는 VM의 알려진 위치에 저장됩니다. [VM의 사용자 지정 데이터에 대한 자세한 정보](#)

사용자 지정 데이터

검토 + 만들기

< 이전

다음: 태그 >

- N. [유효성 검사 통과]를 확인하고 [만들기]를 클릭한다.

가상 머신 만들기 ...

✔ 유효성 검사 통과

기본 사항 디스크 네트워킹 관리 고급 태그 검토 + 만들기

제품 정보

표준 DS2 v2
Microsoft별
[사용 약관](#) | [개인 정보 취급 방침](#)

구독 크레딧 적용 ⓘ
185.5673KRW/시간
[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](#)

만들기

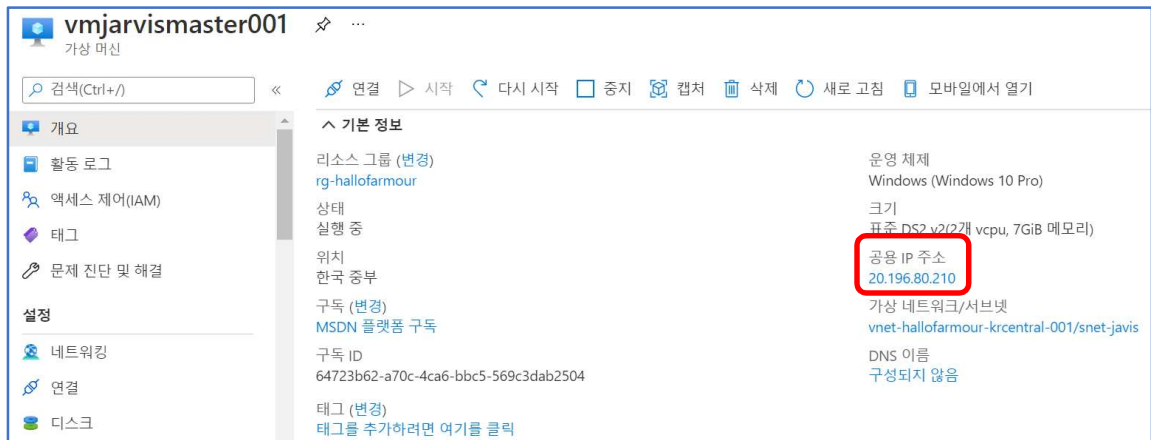
< 이전

다음 >

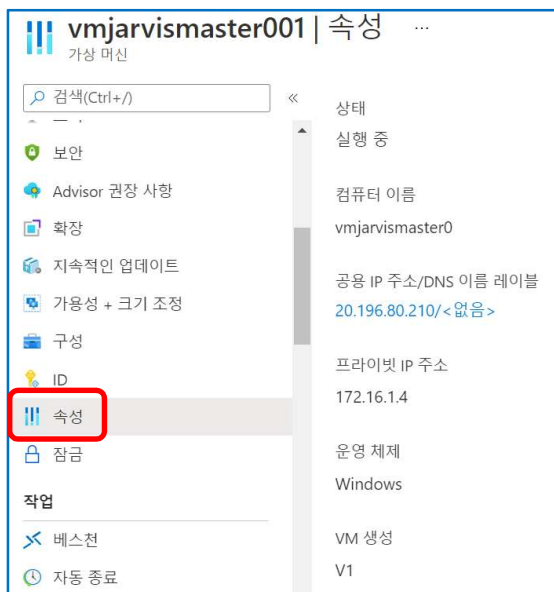
[자동화에 대한 템플릿 다운로드](#)

4. 가상 머신 연결하기

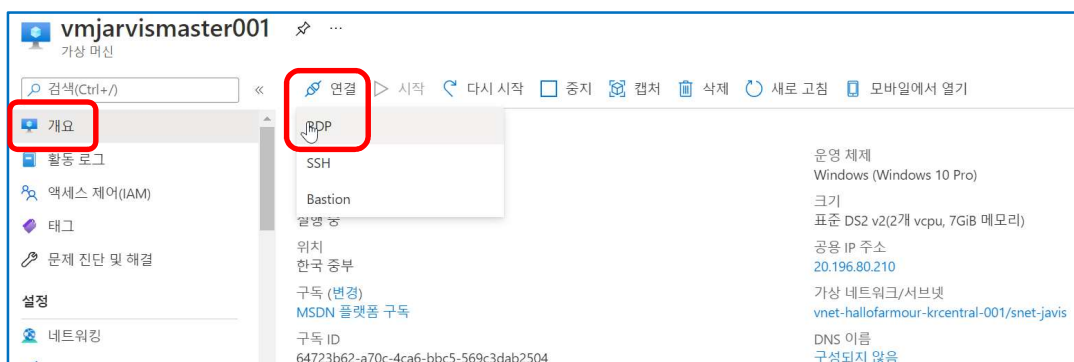
- A. 가상 머신의 생성 및 배포가 모두 완료되면 **rg-hallofarmour** 리소스 그룹에 속해있는 **vmjarvismaster001**을 클릭하여 선택한다. 리소스 메뉴의 **[개요]**가 선택되고, 방금 생성한 가상 머신의 기본 정보를 확인할 수 있다. **[공용 IP 주소]**를 확인할 수 있다.



- B. 리소스 메뉴의 **[속성]**을 선택하면 더 자세한 정보를 확인할 수 있다.



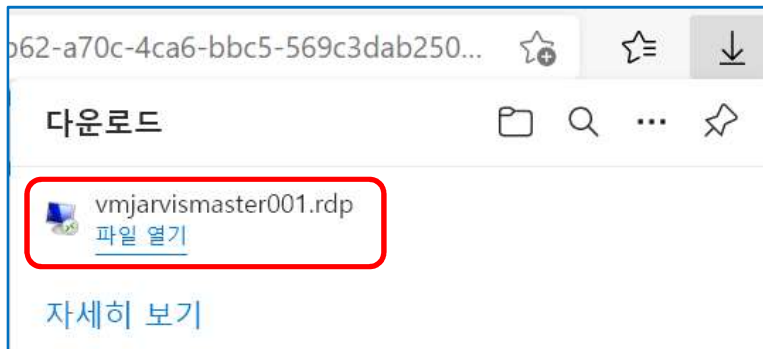
- C. 다시 **[개요]**를 클릭하여 기본 정보 블레이드로 돌아온 뒤, 명령바에서 **[연결]** > **[RDP]**를 선택한다.



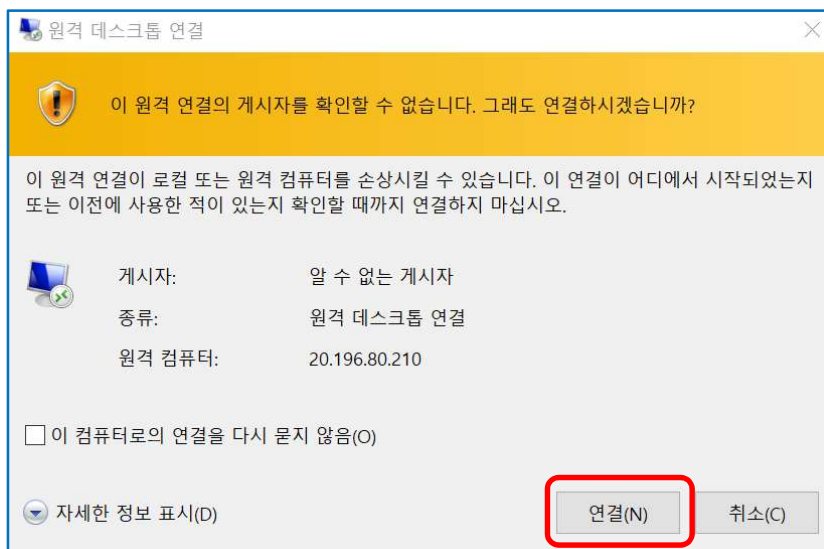
- D. [RDP를 사용하여 연결] 섹션에서 [IP 주소]와 [포트 번호]를 확인하고 [RDP 파일 다운로드]를 클릭한다.



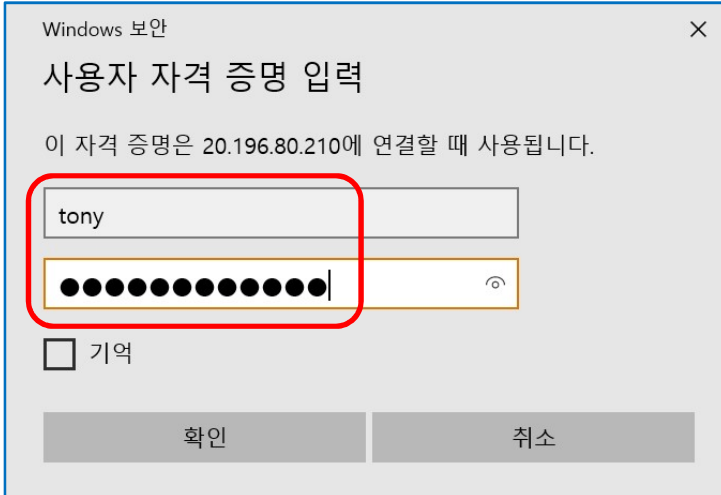
- E. 다운로드한 파일 **vmjarvismaster001.rdp**를 파일 열기 혹은 더블클릭한다.



- F. [원격 데스크톱 연결]창이 나타난다. 연결을 위해 [연결] 버튼을 클릭한다.



- G. [사용자 자격 증명 입력]창에서 이미 가상 머신 생성시 입력했던 아이디 **tony**와 비밀번호 **P@\$W0rd1234**를 입력하고 [확인] 버튼을 클릭한다.



Windows 보안

사용자 자격 증명 입력

이 자격 증명은 20.196.80.210에 연결할 때 사용됩니다.

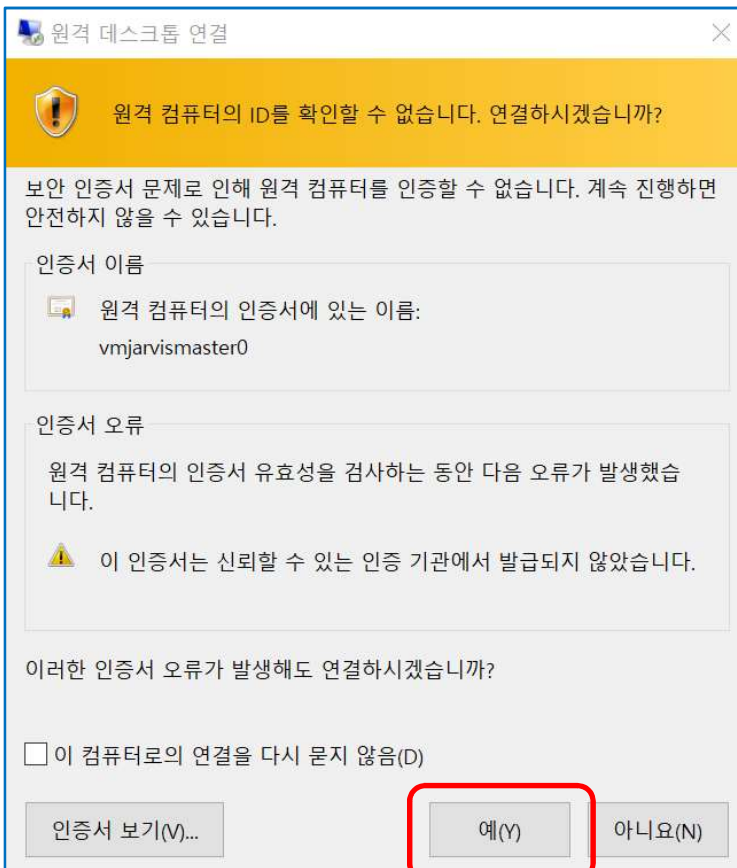
tony

●●●●●●●●●●●●●●●●


☐ 기억

확인 취소

- H. 인증서 경고창이다. 이 인증서는 방금 개별적으로 만들었기 때문에 시스템 입장에서는 신뢰할 수 없는 것이 당연하다. 연결하기 위해 [예(Y)]를 클릭한다.




원격 데스크톱 연결

 원격 컴퓨터의 ID를 확인할 수 없습니다. 연결하시겠습니까?


보안 인증서 문제로 인해 원격 컴퓨터를 인증할 수 없습니다. 계속 진행하면 안전하지 않을 수 있습니다.

인증서 이름

 원격 컴퓨터의 인증서에 있는 이름:
vmjarvismaster0

인증서 오류

원격 컴퓨터의 인증서 유효성을 검사하는 동안 다음 오류가 발생했습니다.

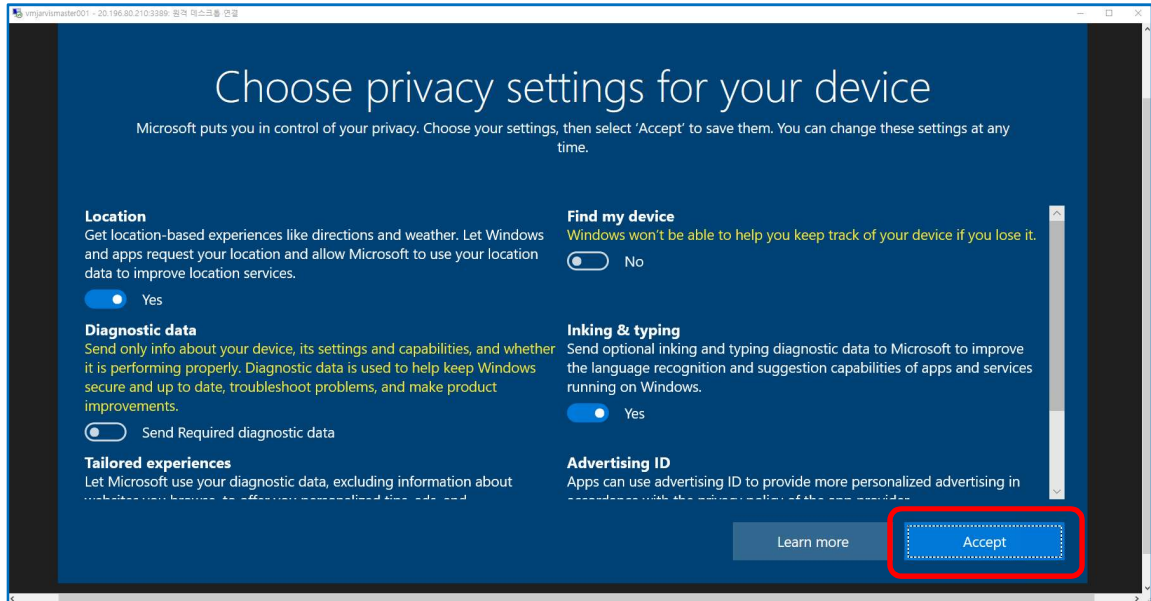
 이 인증서는 신뢰할 수 있는 인증 기관에서 발급되지 않았습니다.

이러한 인증서 오류가 발생해도 연결하시겠습니까?

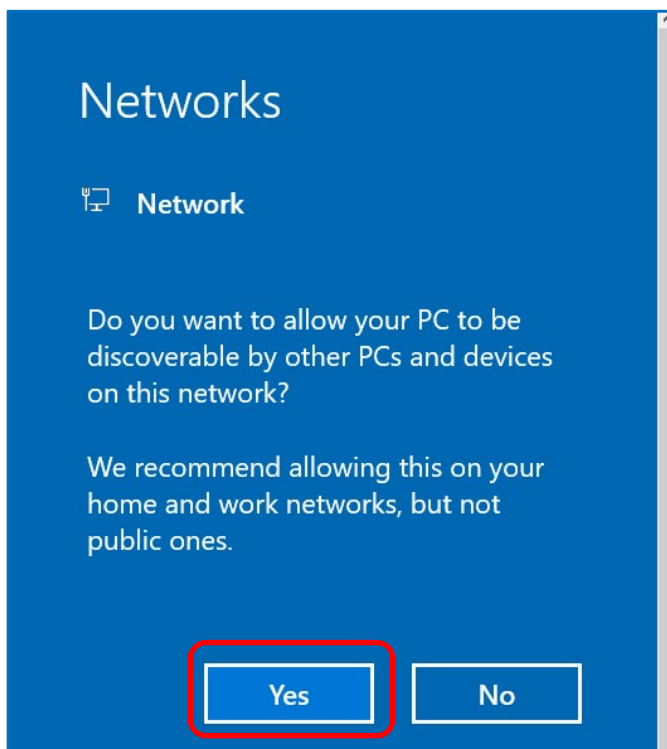
☐ 이 컴퓨터로의 연결을 다시 묻지 않음(D)

인증서 보기(V)... **예(Y)** 아니요(N)

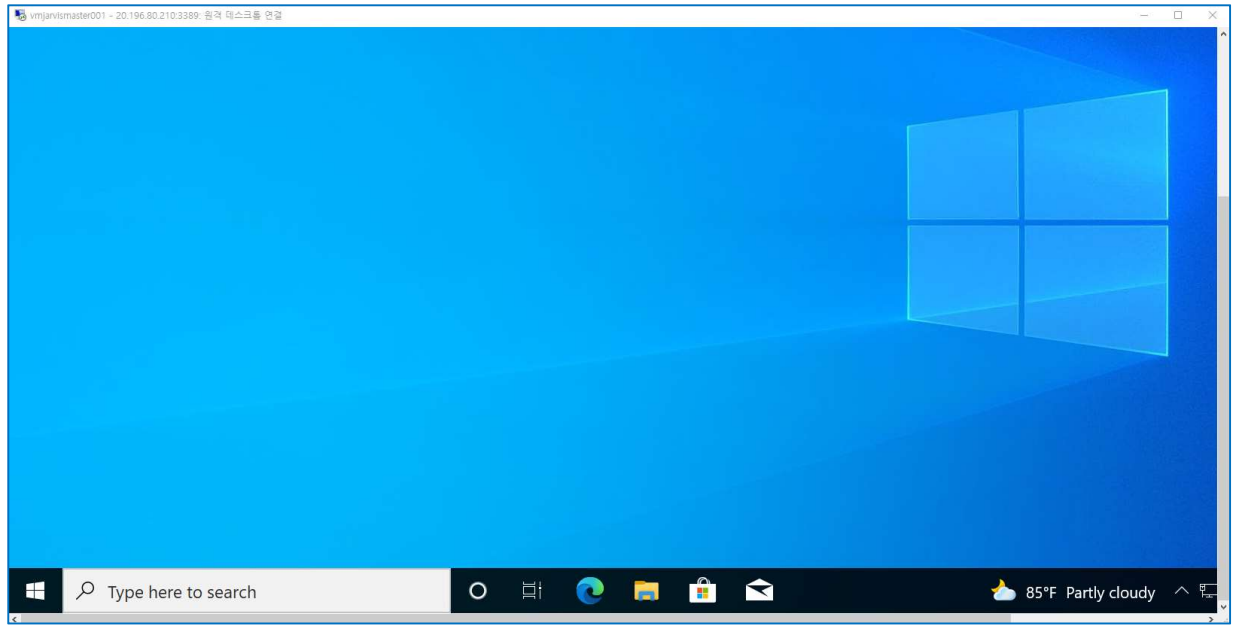
- I. 원격으로 가상 머신과 연결이 성공하면, 다음 그림과 같이 **[Choose privacy settings for your device]** 창이 나타나고 여기서 **[Accept]** 버튼을 클릭한다.



- J. **[Networks]**창에서 **[Yes]**를 선택한다.

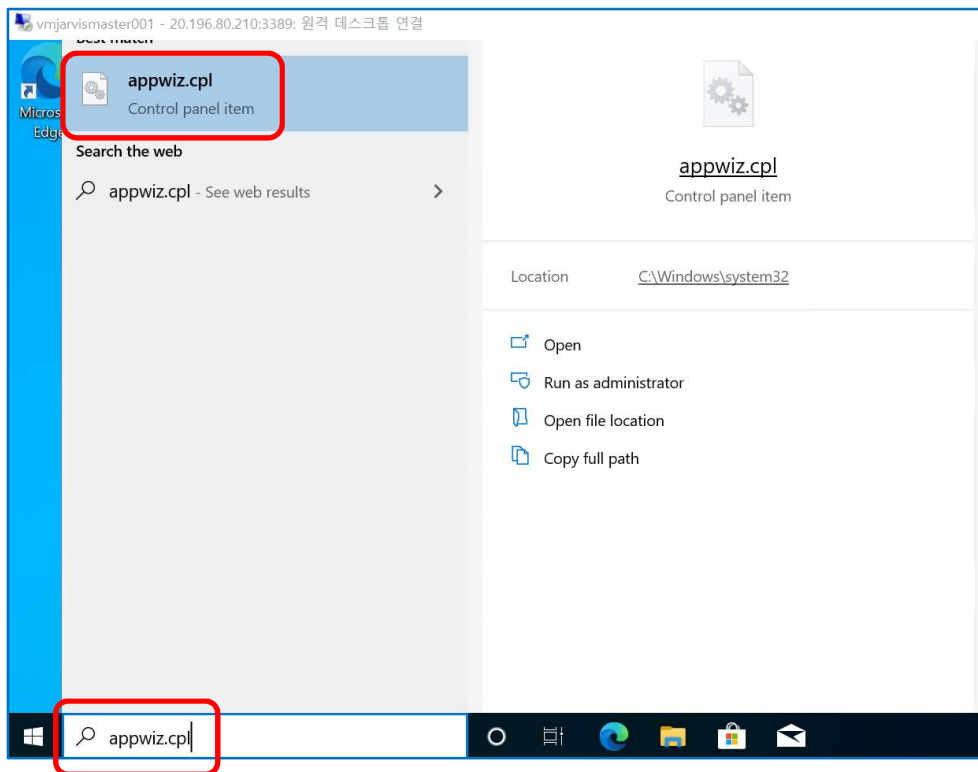


K. 가상 머신의 원격 연결이 성공했다.

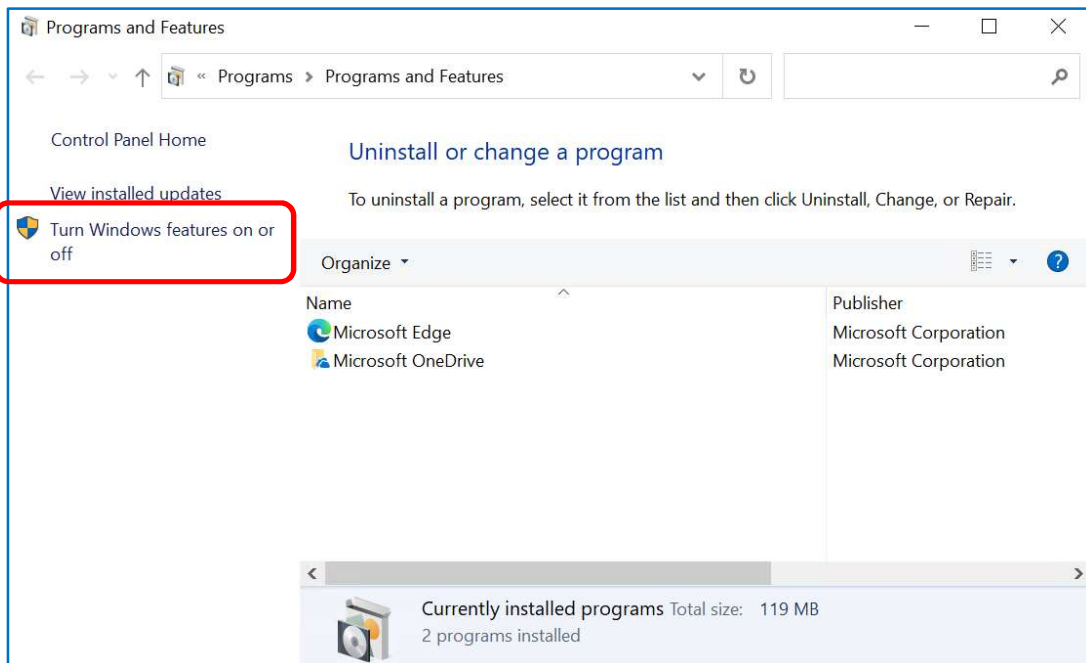


5. Windows 10 가상 머신에 WSL2를 이용한 Ubuntu Server 설치하기

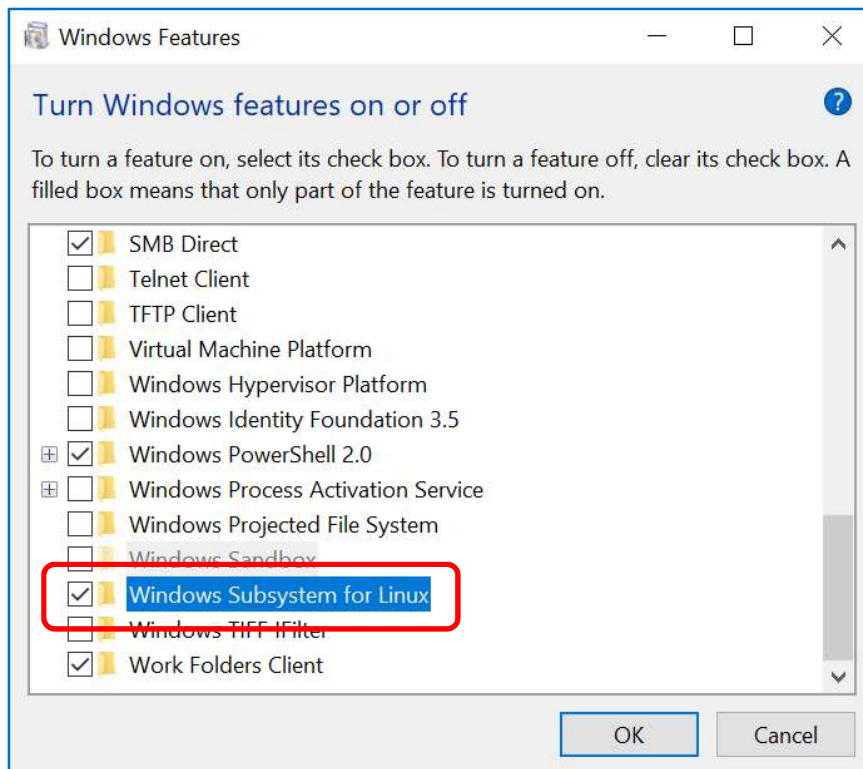
A. 가상 머신 검색창에 **appwiz.cpl** 즉 **프로그램 제거 또는 변경**을 검색하여 해당 프로그램을 선택한다.



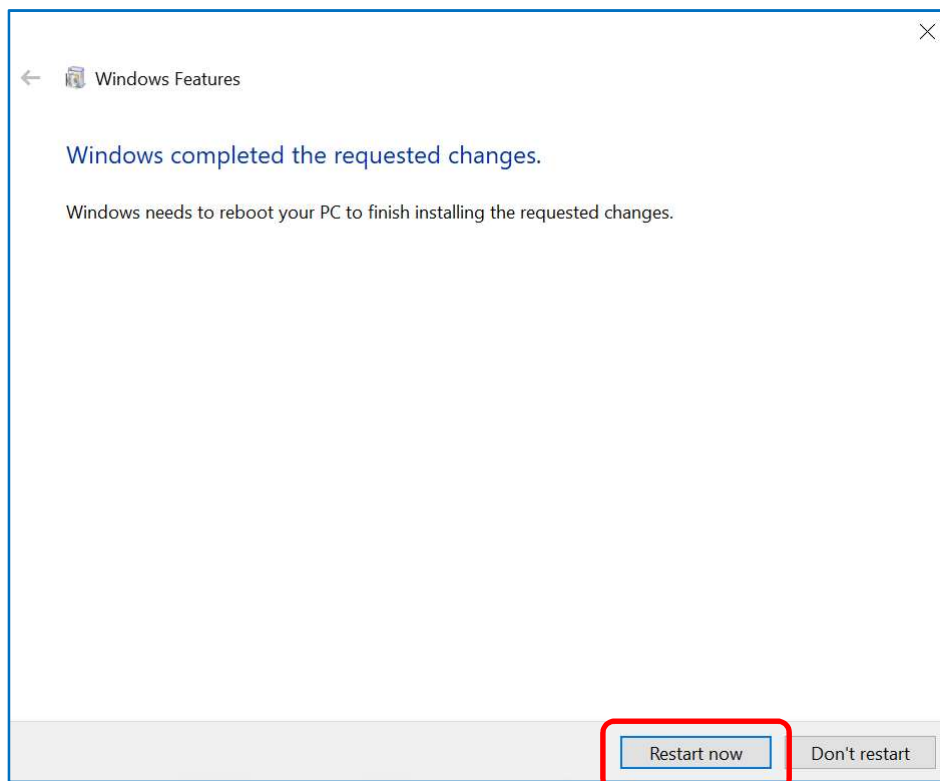
B. 좌측메뉴에서 **[Turn Windows features on or off]**를 선택한다.



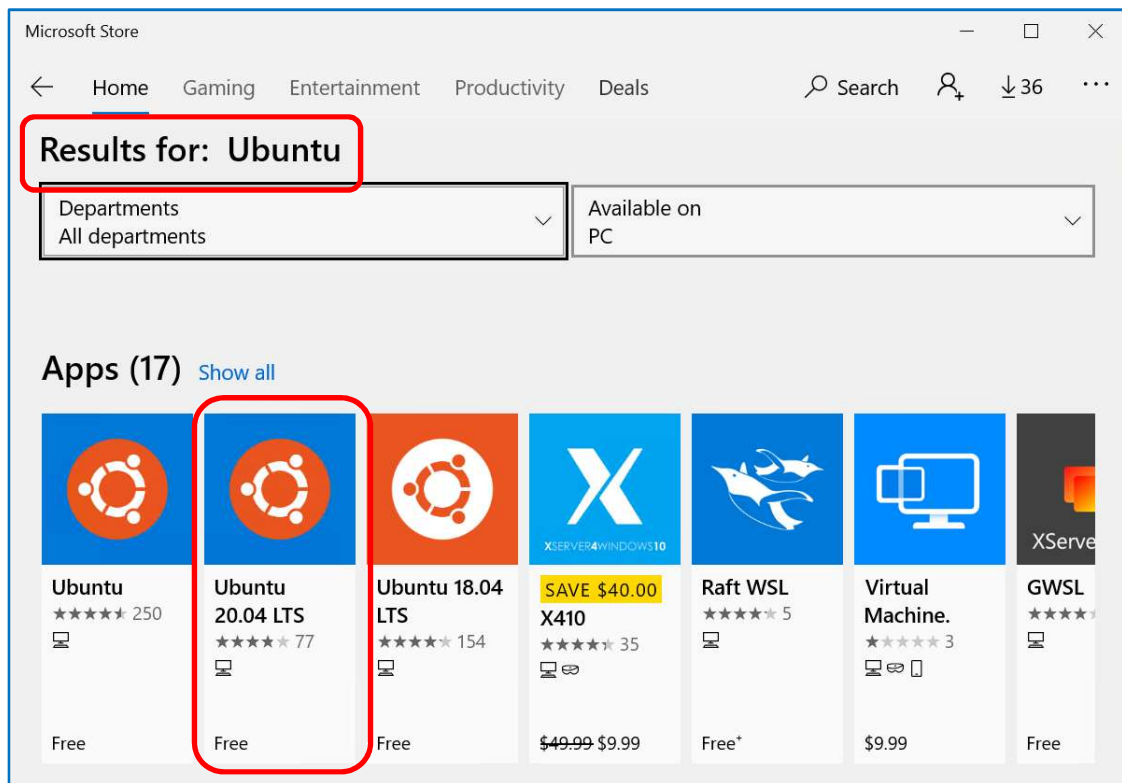
- C. 목록에서 **[Windows Subsystem for Linux]**를 찾아서 체크하고 **[OK]** 버튼을 클릭한다.



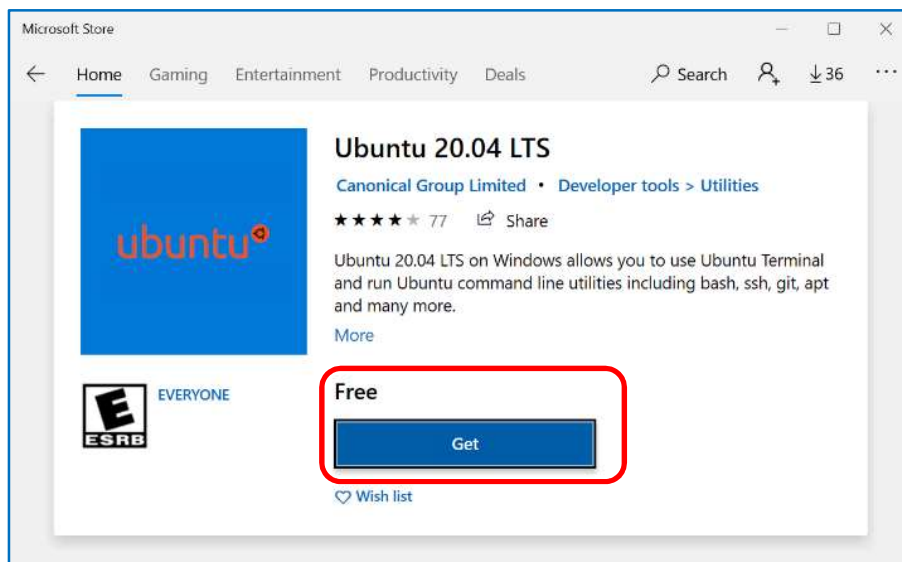
- D. 설치가 모두 끝나면 **[Restart now]**를 클릭하여 가상 머신을 재부팅한다.



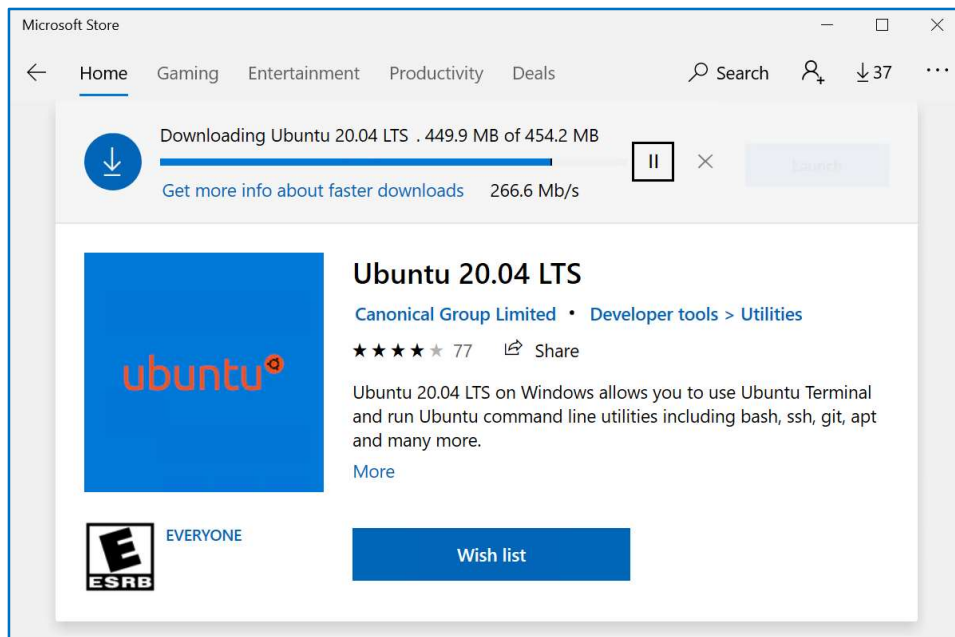
- E. 다시 가상 머신과 연결하여 로그인한다. 가상머신에서 **[Microsoft Store]** 앱을 띄운다음, 검색창에서 **Ubuntu**를 입력한다. 검색 결과에서 Ubuntu 20.04 LTS를 선택한다.



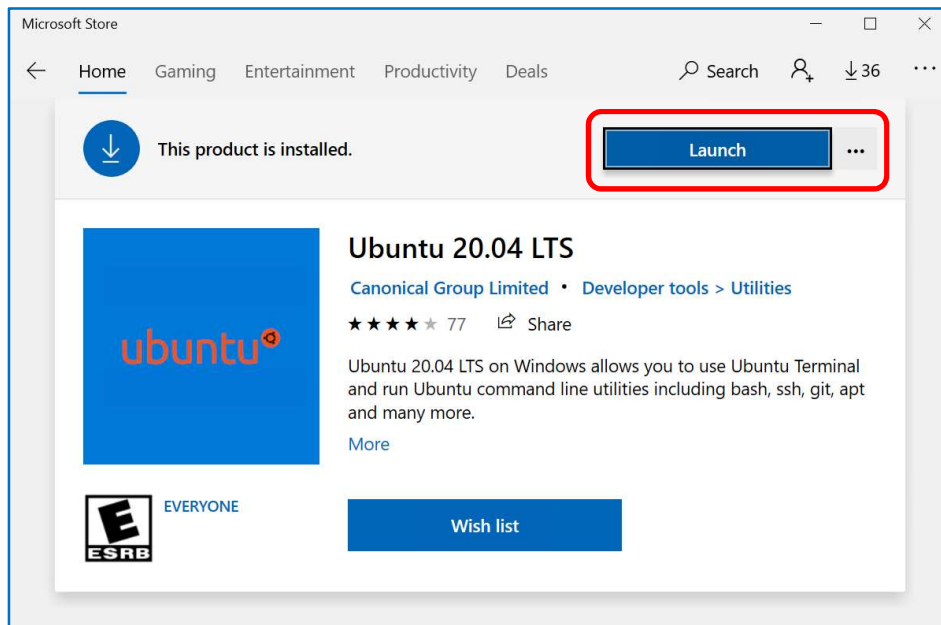
- F. **Ubuntu 20.04 LTS**를 다운로드를 위해 **[Get]** 버튼을 클릭한다.



G. 다운로드 중이다.



H. 다운로드가 끝나면 설치를 위해 [Launch] 를 클릭하면 된다.



- I. 다운로드 받은 **Ubuntu 20.04 LTS** 설치가 모두 마치면 username은 **tony**, Password는 **P@\$\$W0rd1234**를 입력하여 Ubuntu 설치를 모두 마친다.

```
tony@vmjarvismaster0: ~  
Installing, this may take a few minutes...  
Please create a default UNIX user account. The username does not need to match your Windows username.  
For more information visit: https://aka.ms/wslusers  
Enter new UNIX username: tony  
New password:  
Retype new password:  
passwd: password updated successfully  
Installation successful!  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.4.0-19041-Microsoft x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
  
System information as of Wed Jul 14 14:32:25 UTC 2021  
  
System load: 0.52      Processes:            7  
Usage of /home: unknown  Users logged in:      0  
Memory usage: 33%      IPv4 address for eth0: 172.16.1.4  
Swap usage: 0%  
  
1 update can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
This message is shown once a day. To disable it please create the  
/home/tony/.hushlogin file.  
tony@vmjarvismaster0:~$
```