



# Microsoft Cloud Workshop

Azure IaaS 101

Hands-on lab step-by-step

Lab 7

Aug 2018

Moonsun Lee (CSA)

# Contents

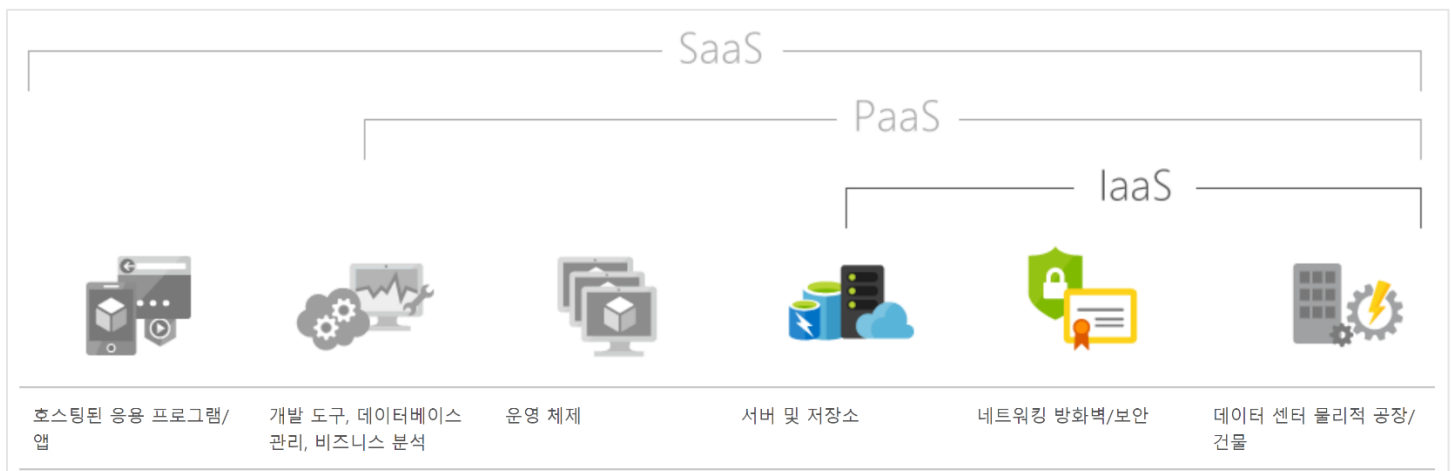
laaS 101 hands-on lab step-by-step.....	1
목표 .....	1
Lab 구성.....	2
요구사항 .....	2
Lab 7: 응용 프로그램 보안 그룹 만들기.....	3
Step 1: 서버넷 및 가상머신 생성.....	3
Step 2: 응용 프로그램 보안 그룹 생성.....	10
Step 3: 응용 프로그램 보안 그룹 구성.....	13
Step 4: 네트워크 보안 그룹 구성 (인바운드 규칙 추가).....	16
Step 5: 검증 시나리오 .....	20

# IaaS 101 hands-on lab step-by-step

## 목표

IaaS(Infrastructure as a Service)는 인터넷을 통해 프로비전 및 관리되는 즉각적인 컴퓨팅 인프라입니다. 수요에 따라 빠르게 강화/규모 축소할 수 있으며 사용한 양만큼만 비용을 지급하면 됩니다.

IaaS 를 사용할 경우 자체 물리적 서버와 기타 데이터 센터 인프라를 구입하고 관리하는 데 따른 비용과 복잡성이 없어집니다. 각 리소스는 별도의 서비스 구성 요소로 제공되며, 특정 리소스를 필요한 동안에만 대여하면 됩니다. 클라우드 컴퓨팅 서비스 공급자는 인프라를 관리하는 반면, 사용자는 자체 소프트웨어(운영 체제, 미들웨어 및 응용 프로그램)를 구매, 설치, 구성 및 관리합니다.



해당 실습은 Azure IaaS(Infrastructure as a Service)를 처음 접해보는 엔지니어를 대상으로 작성되었으며, 실습을 통하여 아래 나열된 Azure 의 IaaS 의 주요 서비스들을 직접 만들어보며 이해할 수 있도록 구성되어 있습니다.

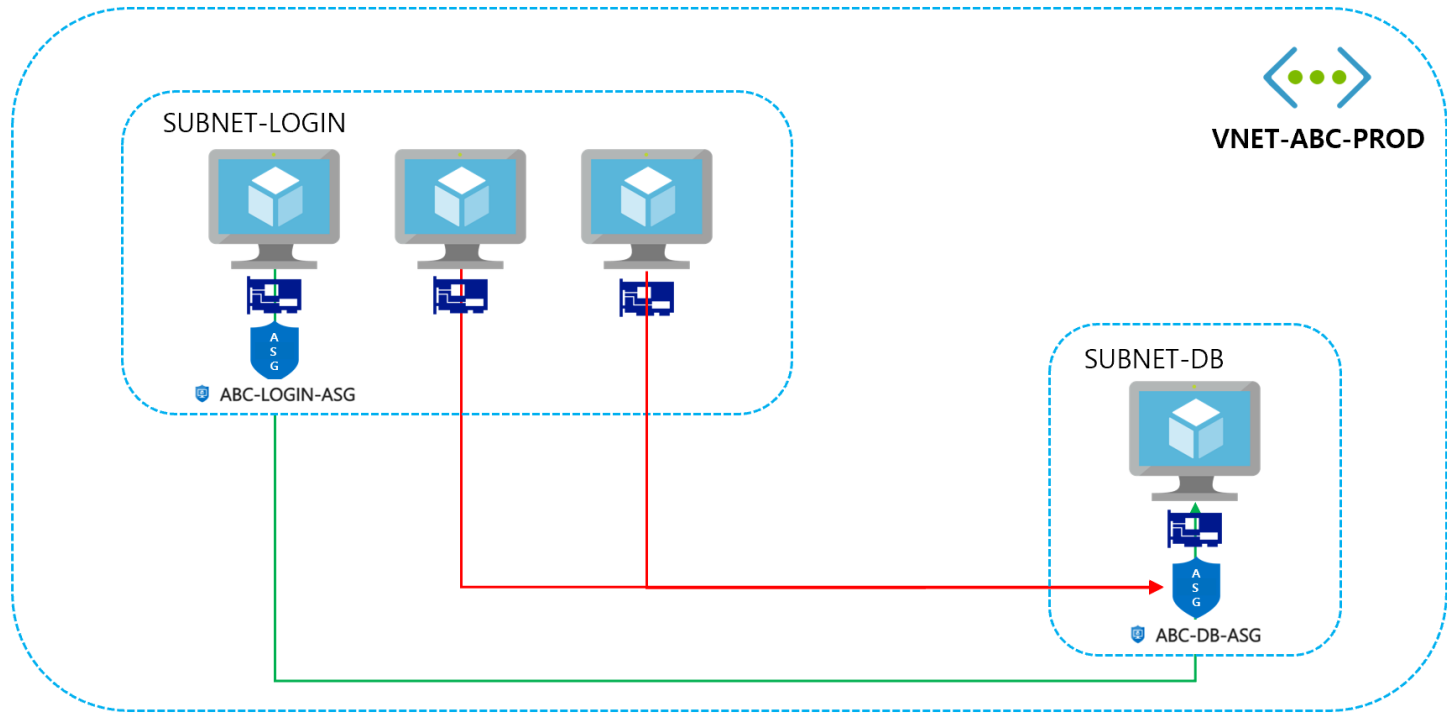
- Azure 가상머신
- Azure 가상네트워크 (서브넷 / 피어링 / 보안)
- Azure VPN 서비스
- Azure 스토리지

## Lab 구성

해당 실습을 마치고 나면, 응용 프로그램 보안 그룹(Azure Application Security Group)을 적용할 수 있습니다. 응용 프로그램 보안 그룹을 사용하면 IP 주소 대신 응용 프로그램에서 중앙 집중식으로 작업 부하를 기반으로 세밀한 네트워크 보안 정책을 정의할 수 있습니다.

- 응용 프로그램 보안 그룹 생성 및 적용

Duration: 30 minutes



우선 순위	이름	포트	프로토콜	소스	대상 주소	작업
1000	Allow-RDP-from-Login	3389	모두	ABC-LOGIN-ASG	ABC-DB-ASG	허용
1010	Deny-RDP-except-LoginASG	3389	모두	모두	ABC-DB-ASG	거부
65000	AllowVnetInBound	모두	모두	VirtualNetwork	VirtualNetwork	허용
65001	AllowAzureLoadBalancerInBound	모두	모두	AzureLoadBalancer	모두	허용
65500	DenyAllInBound	모두	모두	모두	모두	거부

## 요구사항

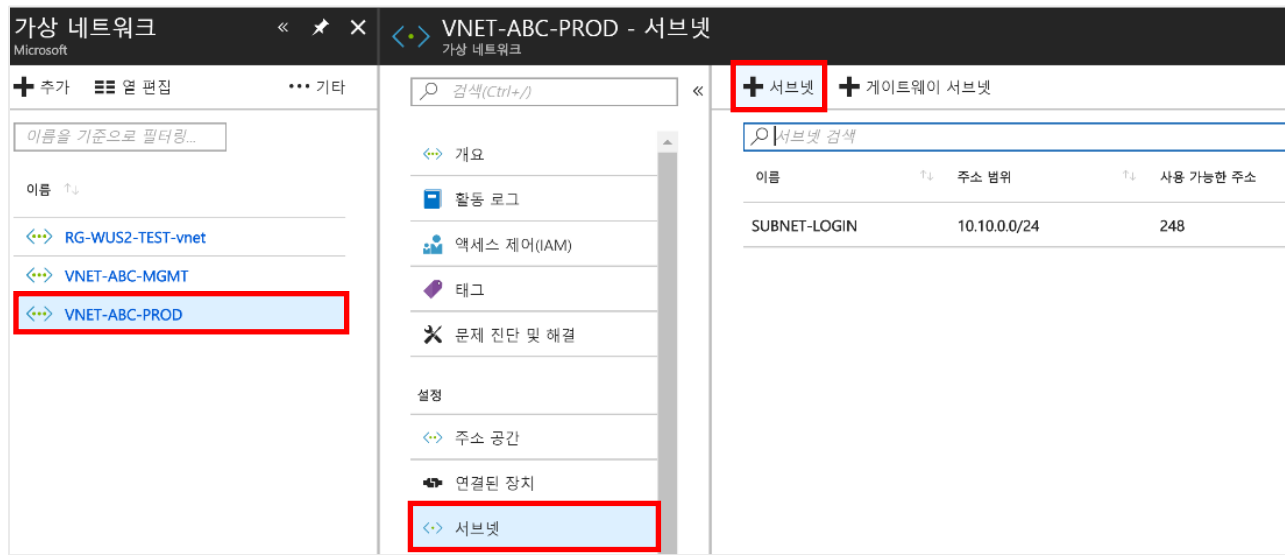
- Microsoft Azure subscription
- Local machine
- Lab01 – 06 실습

## Lab 7: 응용 프로그램 보안 그룹 만들기

### Step 1: 서브넷 및 가상머신 생성

가상 네트워크 "VNET-ABC-PROD"에 새로운 서브넷 "SUBNET-DB"를 생성하고, 내부에 새로운 가상머신을 생성합니다.

1. "VNET-ABC-PROD" 가상 네트워크 서비스 페이지로 이동하여, 서브넷 메뉴로 이동합니다. "+서브넷" 버튼을 클릭하여 새로운 서브넷 "SUBNET-DB"를 생성합니다.



이름 → SUBNET-DB, 주소 범위 → 10.10.1.0/24

\* 이름

SUBNET-DB ✓

\* 주소 범위(CIDR 블록) ⓘ

10.10.1.0/24

10.10.1.0 - 10.10.1.255(Azure 예약된 주소 251 + 5)

네트워크 보안 그룹

없음 >

경로 테이블

없음 >

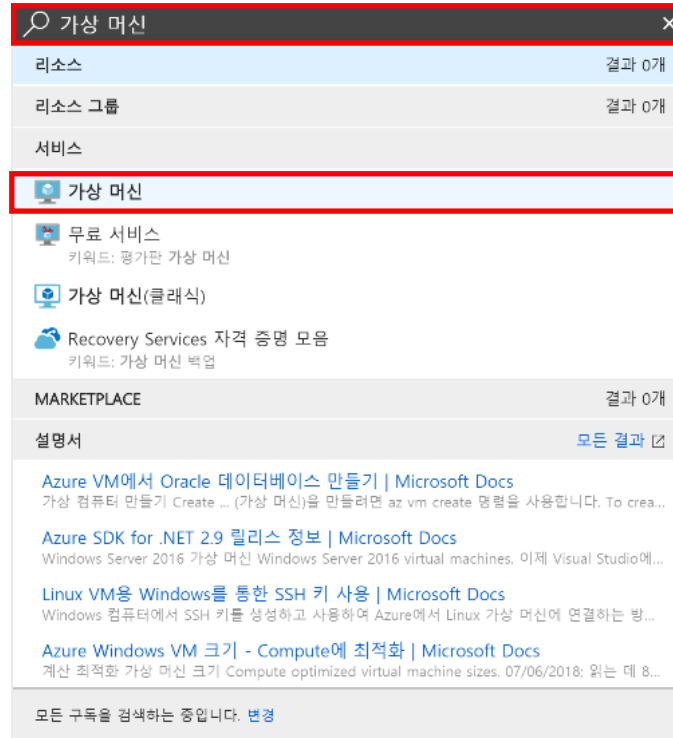
서비스 엔드포인트

서비스 ⓘ

0개 선택됨 ▾

확인

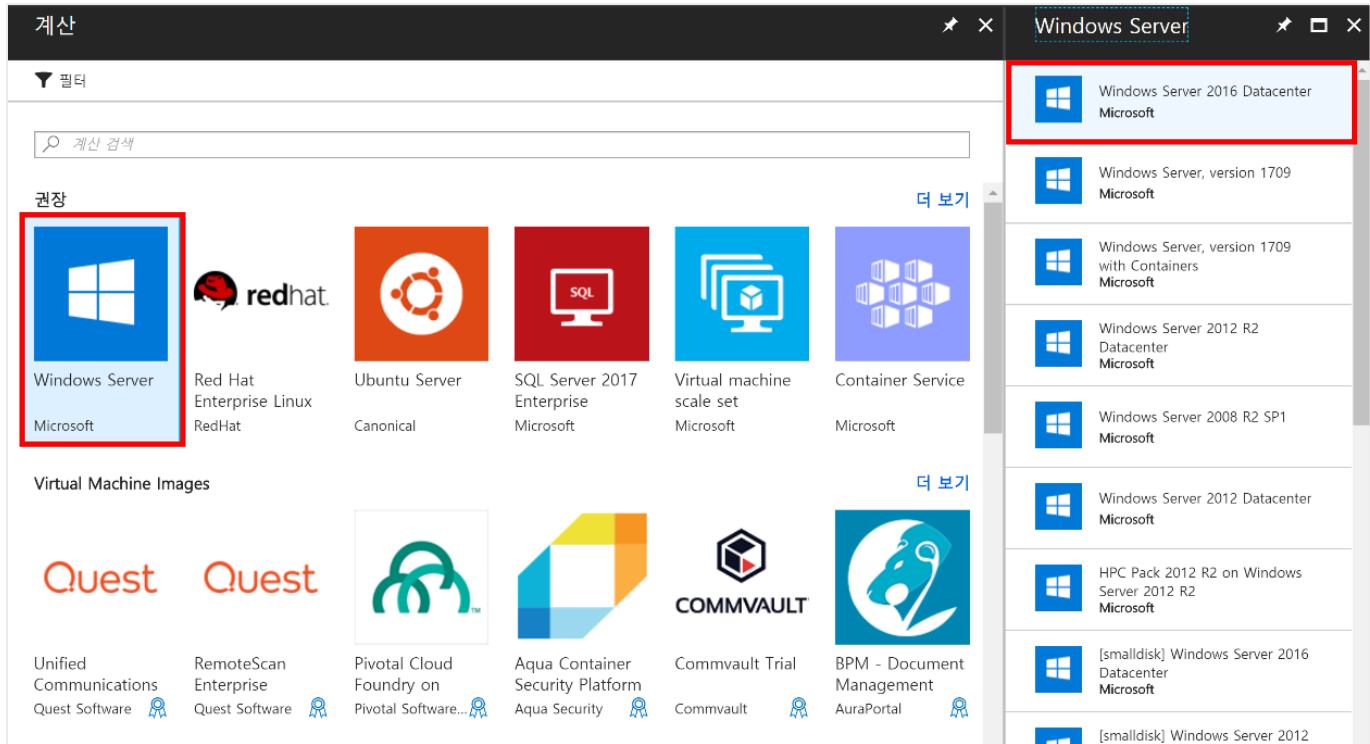
2. 서브넷 생성이 완료되면, 해당 서브넷에 가상머신을 생성합니다. 가상머신 서비스 페이지로 이동합니다.



3. "추가" 버튼을 눌러 새로운 가상머신을 생성합니다.



## 4. 운영체제로 Windows Server 2016 을 선택합니다.



## 5. 만들기 버튼을 클릭하여, 가상머신의 정보를 입력합니다.

Windows Server 2016 Datacenter

Microsoft

Windows Server 2016 is a comprehensive server operating system designed to run the applications and infrastructure that power your business. It includes built-in layers of security and innovation to help you run traditional and cloud-native applications with confidence. This Server with Desktop Experience image includes all roles including the graphical user interface (GUI).

This image can be used with [Azure Hybrid Benefit for Windows Server](#).

**Legal Terms**

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

♡

나중에 위해 저장

게시자	Microsoft
유용한 링크	<a href="#">Documentation</a> <a href="#">Introducing Windows Server 2016</a> <a href="#">What's New in 2016</a> <a href="#">Learn more</a>

배포 모델 선택 ⓘ

Resource Manager

만들기

6. "SUBNET-DB"에 생성될 가상머신의 기본 정보를 입력합니다.

- 이름 → **ABC-DB-PRD01**
- 사용자 이름 → **azureadmin**
- 암호 → **Password@123**
- 리소스그룹 → **RG-VM-PROD**
- 위치 → **미국 서부 2**
- VM 크기 → **D2s\_v3 ( 2 vCores / 8 GB )**

**가상 머신 만들기**

새 만들기 환경 미리 보기 →

- 1 기본 사항  
기본 설정 구성
- 2 크기  
가상 머신 크기 선택
- 3 설정  
옵션 기능 구성
- 4 요약  
Windows Server 2016 Datacenter...

**기본 사항**

\* 이름: ABC-DB-PRD01 ✓

VM 디스크 유형: SSD

\* 사용자 이름: azureadmin ✓

\* 암호: Password@123 ✓

\* 암호 확인: Password@123 ✓

구독: Visual Studio Enterprise

\* 리소스 그룹: RG-VM-PROD (기존 그룹 사용) ✓

\* 위치: 미국 서부 2 ✓

비용 절감

**확인**

B8ms	표준	범용	8	32	16	10800	64 GB	SSD	1,2,3	₩314,614
D2s_v3	표준	범용	2	8	4	4000	16 GB	SSD	1,2,3	₩80,327
★ D4s_v3	표준	범용	4	16	8	8000	32 GB	SSD	1,2,3	₩160,654
D8s_v3	표준	범용	8	32	16	16000	64 GB	SSD	1,2,3	₩321,308

제시된 가격은 Azure 인프라 비용과 구독 및 위치에 대한 할인만 포함된 현지 통화 단위의 예상액입니다. 가격에는 적용 가능한 소프트웨어 비용이 포함되어 있지 않습니다. 권장되는 크기는 하드웨어 및 소프트웨어 요구 사항에 따라 선택한 이미지의 게시자가 결정합니다.

**선택**



7. 가상머신에 Lab 3 에서 미리 생성해둔 설정 정보를 입력합니다.

- 가용성 집합 → 없음
- 가상 네트워크 → VNET-ABC-PROD
- 서브넷 → SUBNET-DB
- 네트워크 보안 그룹 → 포트허용 안함
- 자동 종료 → 켜짐 및 UTC + 09:00(서울)

### 가상 네트워크 선택 → VNET-ABC-PROD 선택

설정

가상 네트워크 선택

고가용성

가용성 영역

없음

\* 가용성 집합

없음

저장소

관리 디스크 사용

아니요

예

네트워크

\* 가상 네트워크

VNET-ABC-PROD

\* 서브넷

SUBNET-LOGIN(10.10.0.0/24)

\* 공용 IP 주소

(새로 만드는 중) ABC-DB-PR...

네트워크 보안 그룹

기본

고급

확인

다음은 선택한 구독 및 '미국 서부 2'에 있는 가상 네트워크입니다.

+

새로 만들기

RG-WUS2-TEST-vnet

RG-WUS2-TEST

VNET-ABC-MGMT

RG-NW-PROD

VNET-ABC-PROD

RG-NW-PROD

## 서브넷 → SUBNET-DB 선택

**설정**

**고가용성**  
가용성 영역  
없음

\* 가용성 집합  
없음

**저장소**  
관리 디스크 사용  
아니오 예

**네트워크**  
\* 가상 네트워크  
VNET-ABC-PROD

\* 서브넷  
SUBNET-DB(10.10.1.0/24)

\* 공용 IP 주소  
(새로 만드는 중) ABC-DB-PR...

**서브넷 선택**

SUBNET-DB  
RG-NW-PROD

SUBNET-LOGIN  
RG-NW-PROD

## 공용 인바운드 포트 없음 선택 / 자동 종료 표준 시간대 (서울) 설정

**설정**

네트워크 보안 그룹  
기본 고급

\* 공용 인바운드 포트 선택  
공용 인바운드 포트 없음  
☒ 공용 인바운드 포트 없음  
☐ HTTP  
☐ HTTPS  
☐ SSH (22)  
☐ RDP (3389)  
☐ MS SQL (1433)

**확장**  
확장  
확장 없음

**자동 종료**  
자동 종료 사용  
끄기 켜기

종료 시간  
오후 7:00:00

표준 시간대  
(UTC+09:00) 서울

**확인**

가상머신의 설정을 모두 마치고, 마지막으로 해당 가상머신의 설정 값/비용 등을 확인할 수 있는 요약 페이지가 나타납니다.  
내가 설정한 값이 맞는지 잘 확인한 뒤, 만들기 버튼을 클릭하여 가상머신을 생성합니다.

가상 머신 만들기

새 만들기 환경 미리 보기 →

1 기본 사항 완료

2 크기 완료

3 설정 완료

4 요약 Windows Server 2016 Datacenter... >

만들기

유�효성 검사 통과

제품 세부 정보

표준 D2s v3 107.9664KRW/시간

Microsoft 제공

약관 | 개인정보처리방침

Azure 리소스

Azure 구독 크레딧 또는 현금 약정 금액 자금을 이용하여 구매할 수 있습니다. 표시된 가격은 소매 가격이며 해당 구독과 연관된 할인이 반영되어 있지 않을 수 있습니다.

요약

기본 사항

구독 Visual Studio Enterprise

리소스 그룹 RG-VM-PROD

약관

“만들기”을(를) 클릭함으로써 나는 (a) 위의 각 Marketplace 제품과 관련된 약관 및 개인정보처리방침에 동의하고, (b) 제품 사용을 중단할 때까지 Microsoft가 현재 결제 방법으로 관련 세금을 비롯해 제품을 사용하는 일과 관련된 요금을 청구하도록 권한을 부여하는 데 동의합니다. 또한 (c) Microsoft가 거래 목적으로 내 연락처 정보와 거래 세부 정보(제품과 관련된 사용량 포함)

☒ Microsoft나 공급자가 이 제품이나 관련 제품과 관련하여 나에게 연락할 수 있도록, 내 연락처 정보를 사용하고 공유할 수 있는 권한을 Microsoft에 부여합니다.

만들기

템플릿 및 매개 변수 다운로드

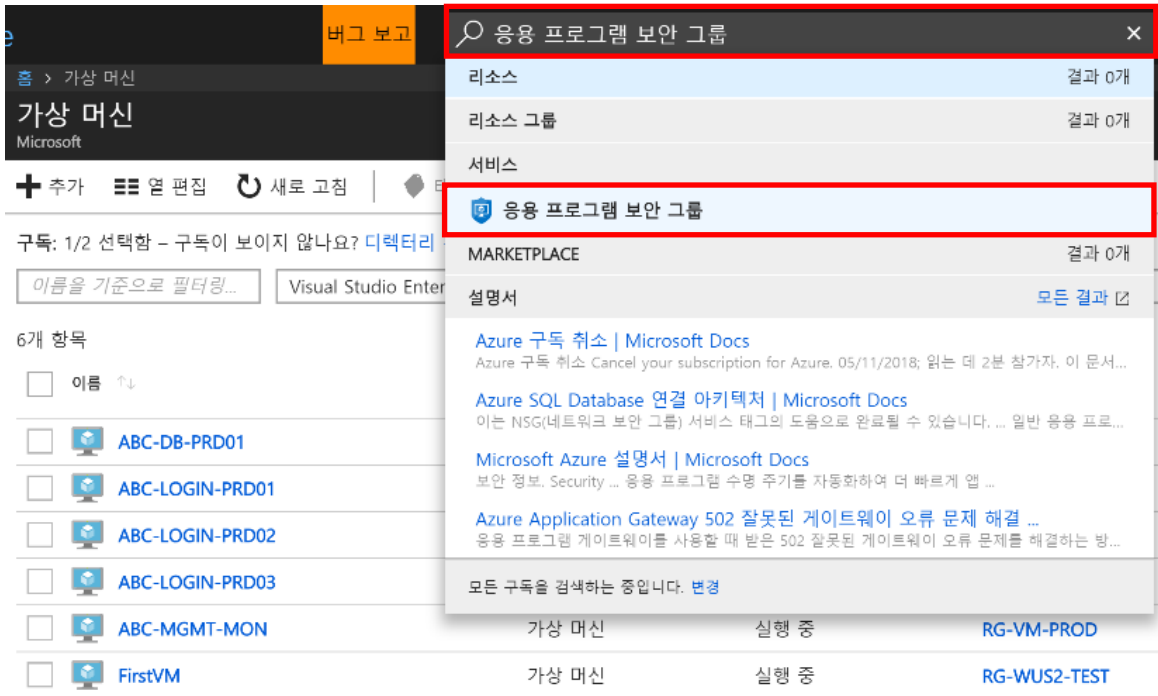
9 | Page

©2018 Microsoft Corporation

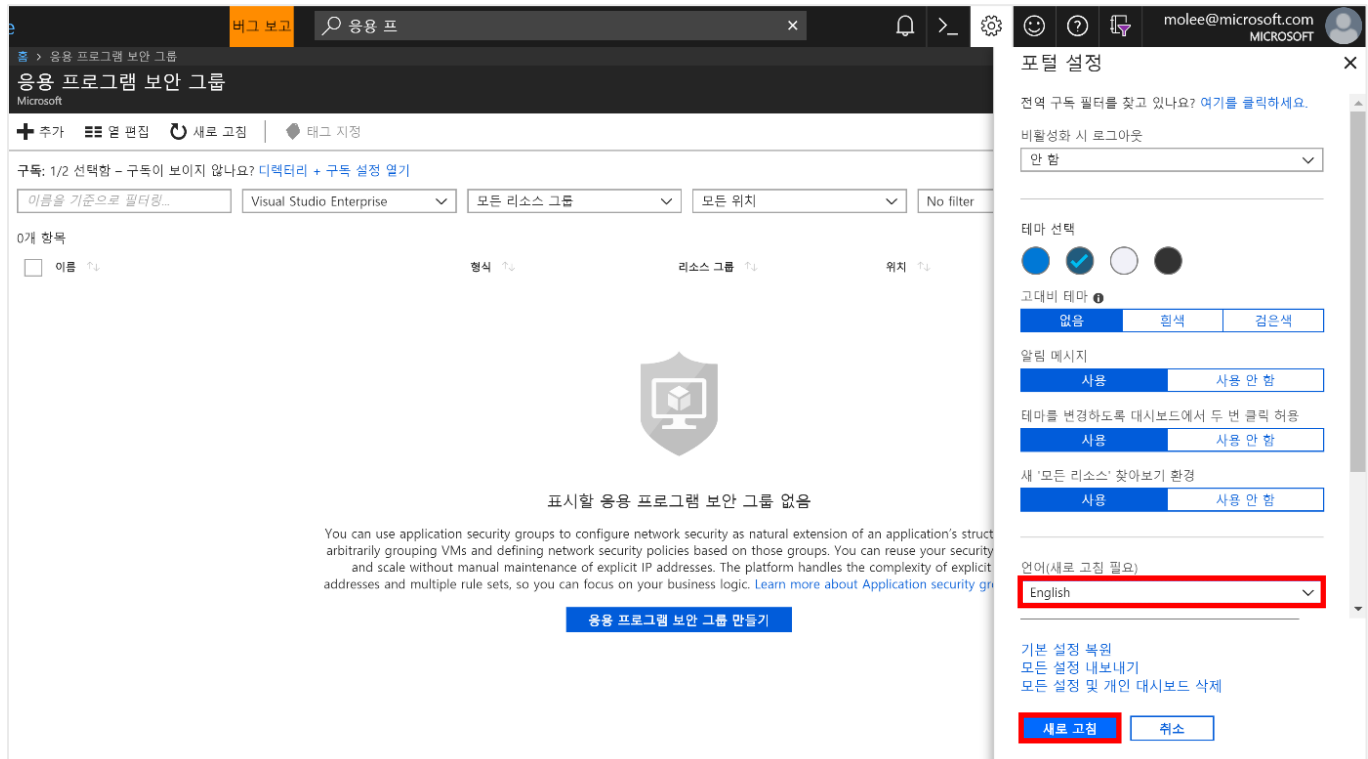
## Step 2: 응용 프로그램 보안 그룹 생성

“ABC-LOGIN-PRD” 가상머신과 “ABC-DB-PRD” 가상머신에 적용될 응용 프로그램 보안 그룹을 생성합니다.

1. 가상머신 생성이 완료되면, 검색창에서 “응용 프로그램 보안 그룹”을 선택하고 서비스 페이지로 이동합니다.



**\*\* 포탈 설정 버튼을 눌러 언어를 영어로 변경합니다. (문서작성 당시, 한국어 언어 버그발생. 포탈 핫픽스 디플로이 예정)\*\***



2. "+추가" 버튼을 클릭하여, LOGIN/DB 가상머신 NIC 에 적용할 응용 프로그램 보안 그룹을 각각 생성합니다.

이름	ABC-LOGIN-ASG	ABC-DB-ASG
리소스 그룹	RG-NW-PROD	RG-NW-PROD
위치	West US 2	West US 2

이름 / 리소스 그룹/ 위치를 입력하고, "만들기" 버튼을 클릭합니다.

Create an application security group

Basic
Tags
Summary

\* Name  
ABC-LOGIN-ASG

\* Subscription  
Visual Studio Enterprise


\* Resource group  
☐ Create new
☒ Use existing  
RG-NW-PROD

\* Location  
West US 2

Review + create
Previous
Next: Tags »
Download a template for automation

다시 "만들기" 버튼을 클릭하여 보안 그룹을 생성합니다.

### Create an application security group

 Success

Basic

Tags

Summary

Summary

Basic

subscription	Visual Studio Enterprise
Resource group	RG-NW-PROD
location	West US 2
name	ABC-LOGIN-ASG

Create

« Previous: Tags

Next

Download a template for automation

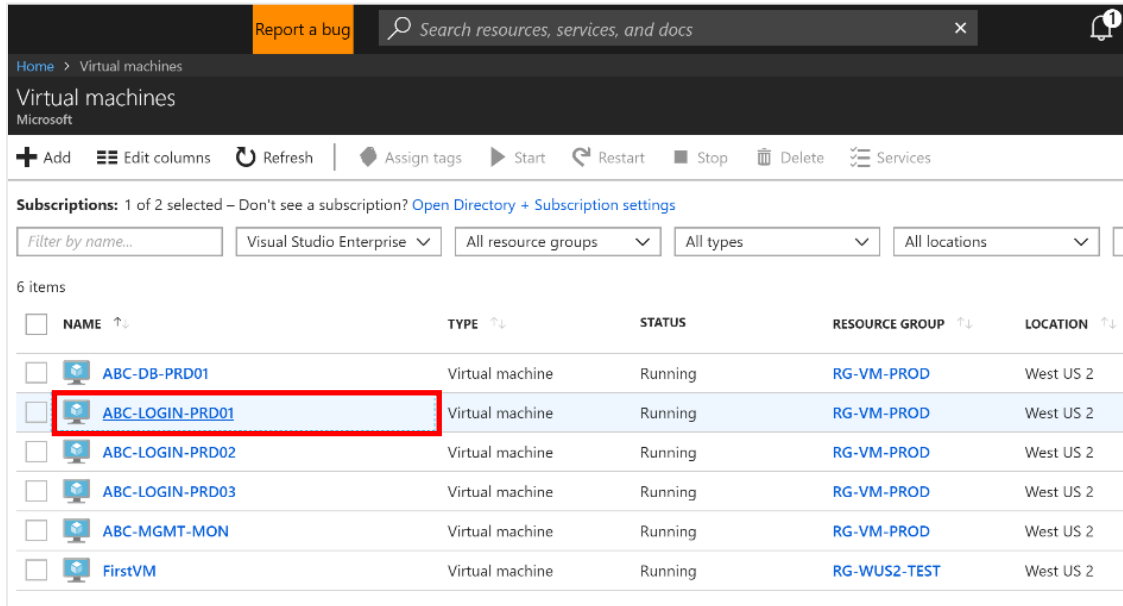
동일한 방법으로 "**ABC-DB-ASG**" 응용 프로그램 보안 그룹도 생성합니다.

Application security groups			
Microsoft			
<div><div>+ Add</div><div>≡ Edit columns</div><div>↺ Refresh</div><div>◆ Assign tags</div></div>			
<b>Subscriptions:</b> 1 of 2 selected – Don't see a subscription? <a href="#">Open Directory</a> + <a href="#">Subscription settings</a>			
<input type="text" value="Filter by name..."/>	<input type="text" value="Visual Studio Enterprise"/>	<input type="text" value="All resource groups"/>	<input type="text" value="All locations"/>
2 items			
<input type="checkbox"/>	NAME ↑↓	TYPE ↑↓	RESOURCE GROUP ↑↓
<input type="checkbox"/>	ABC-DB-ASG	Application security group	RG-NW-PROD
<input type="checkbox"/>	ABC-LOGIN-ASG	Application security group	RG-NW-PROD
	LOCATION ↑↓		

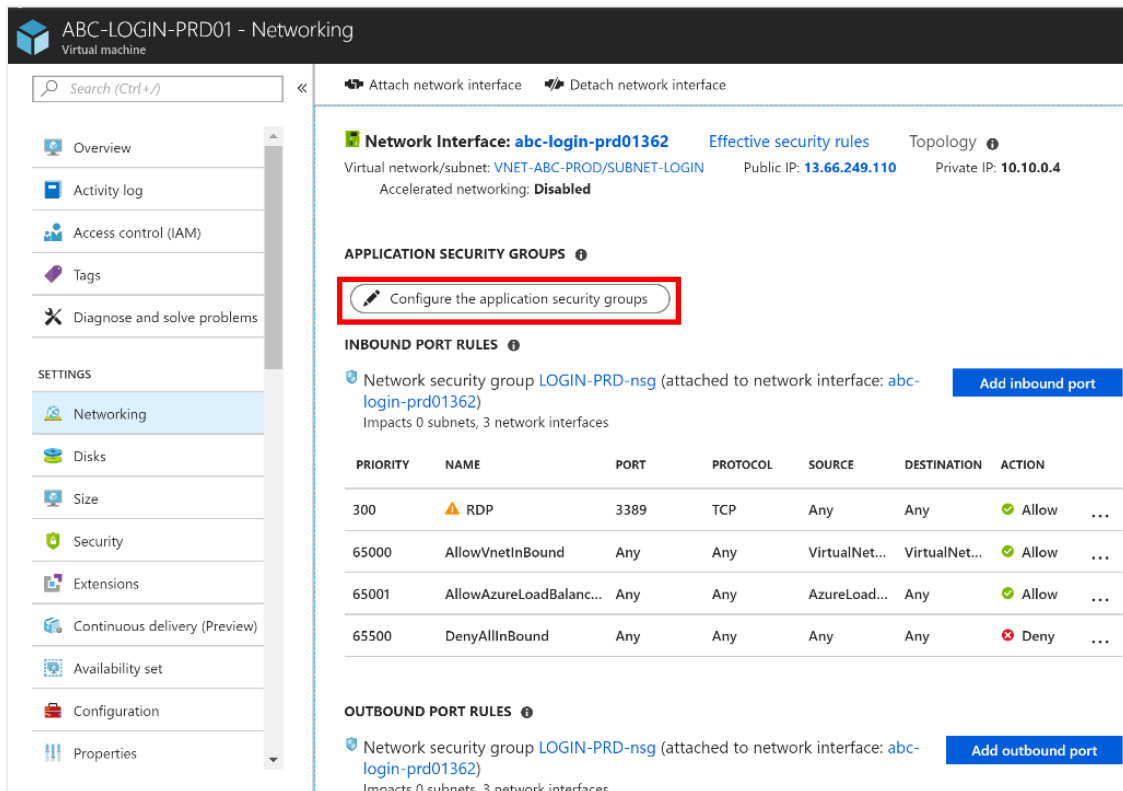
## Step 3: 응용 프로그램 보안 그룹 구성

“ABC-LOGIN-PRD01” 가상머신과 “ABC-DB-PRD” 가상머신의 NIC 에 위에서 생성한 응용 프로그램 보안 그룹을 추가하여, 해당 보안 그룹의 적용을 받을 수 있도록 합니다.

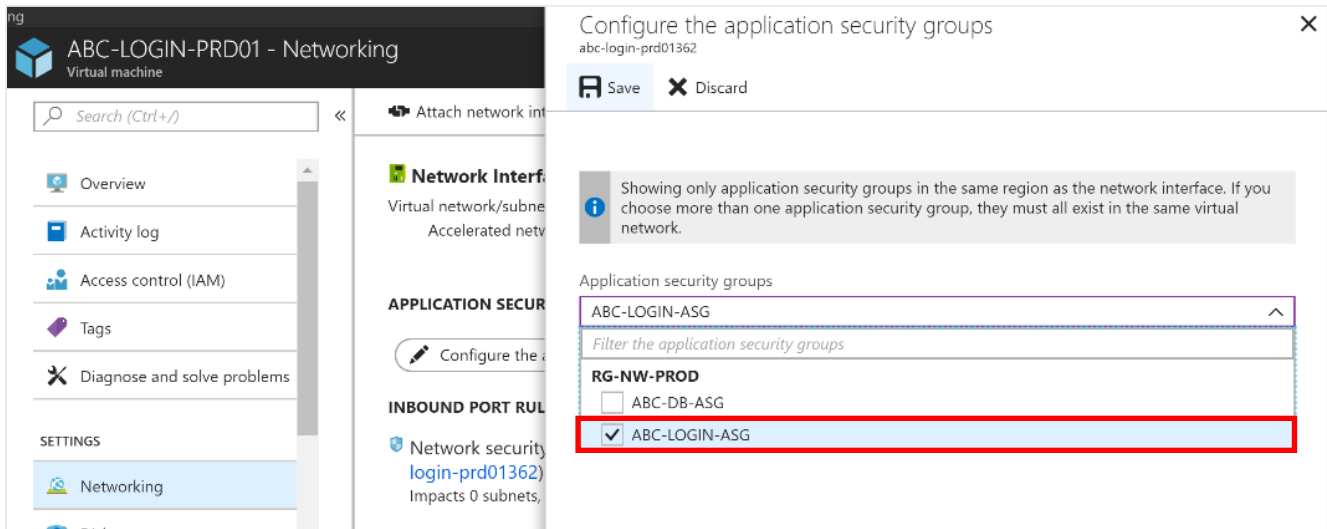
1. “가상 머신” 서비스 페이지로 이동하여, **ABC-LOGIN-PRD01** 가상머신 상세 페이지로 이동합니다.



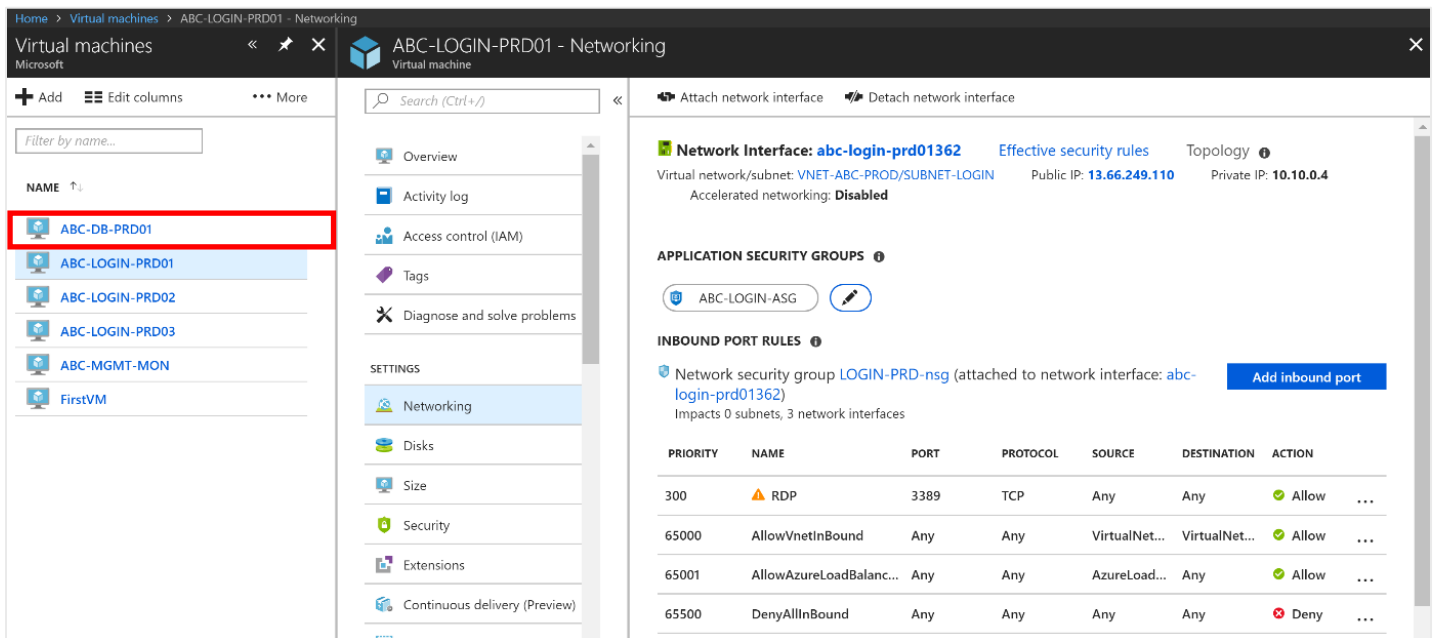
2. 네트워크 메뉴로 이동하여, 응용 프로그램 보안 그룹 구성하기 버튼을 클릭합니다.



3. 위에서 생성한 **ABC-LOGIN-ASG** 보안 그룹을 선택하고, 저장합니다. 이제 **ABC-LOGIN-PRD01** 가상머신은 해당 보안그룹의 적용을 받습니다.

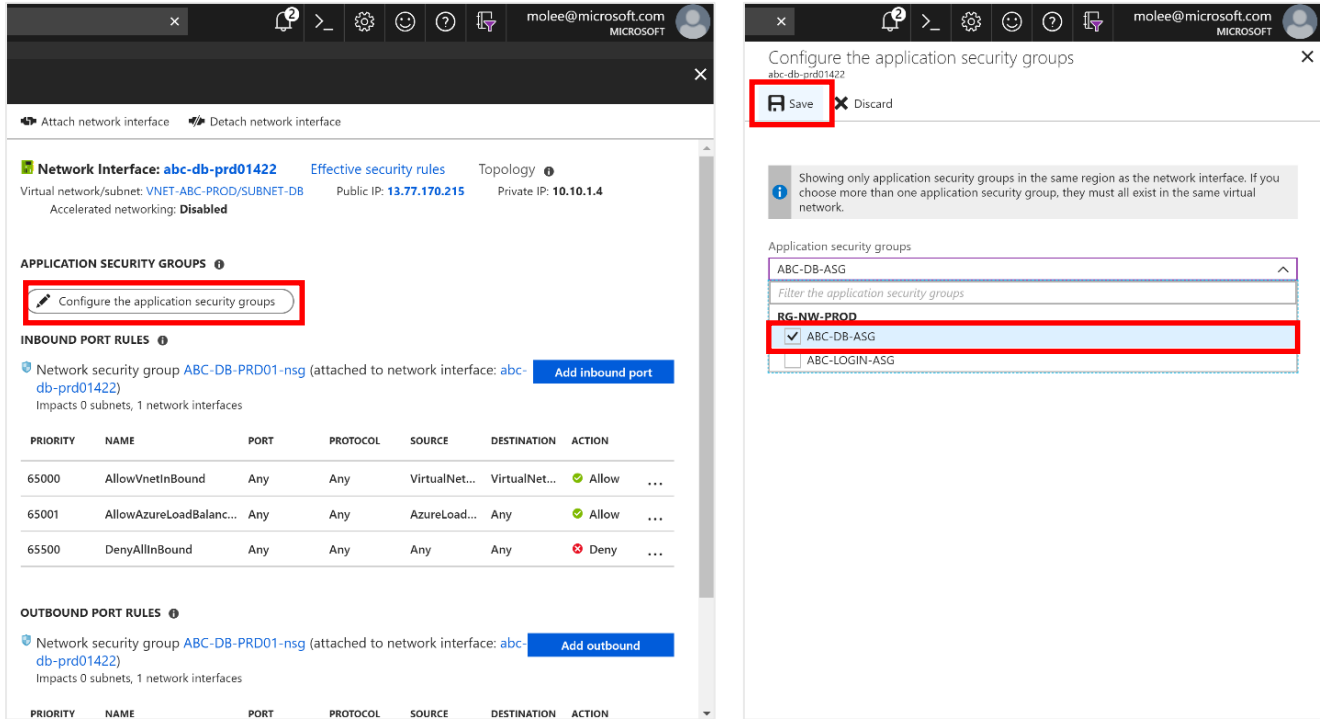


4. **ABC-DB-PRD01** 가상 머신으로 이동하여, 동일한 방법으로 **ABC-DB-ASG** 보안 그룹을 적용합니다.

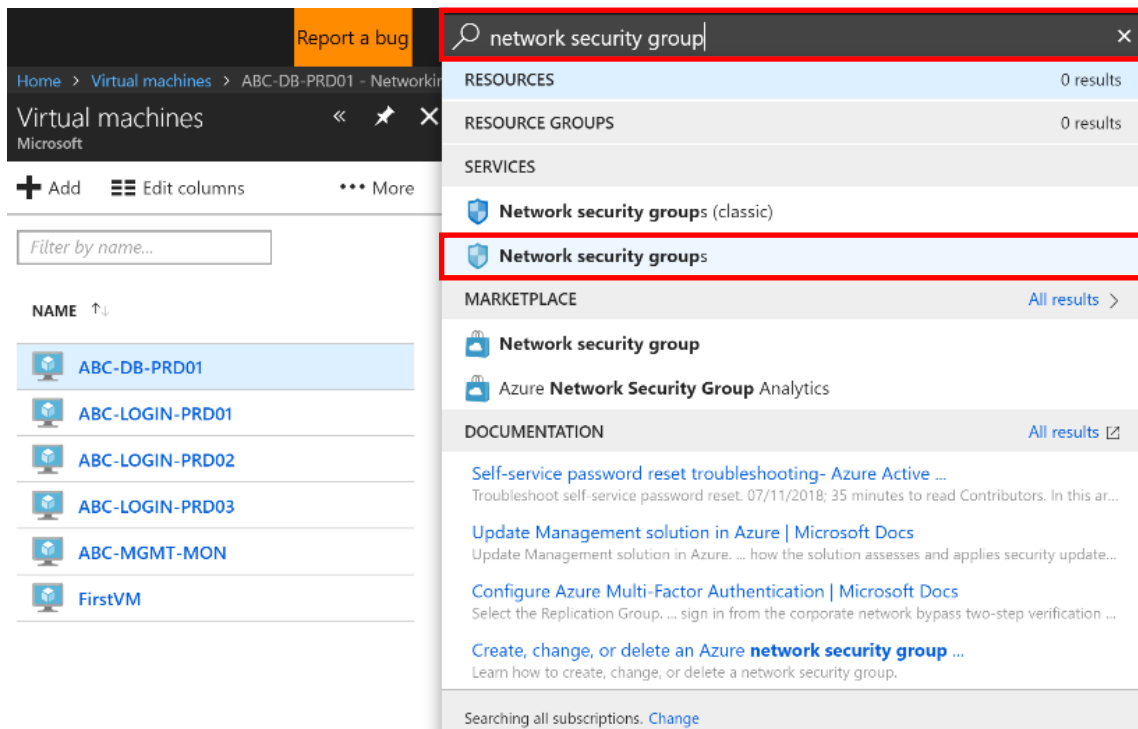




5. 응용 프로그램 보안 그룹 구성하기 버튼을 클릭한 뒤, 위에서 생성한 **ABC-DB-ASG** 보안 그룹을 선택하고 저장합니다. 이제 **ABC-DB-PRD01** 가상머신은 해당 보안그룹의 적용을 받습니다.



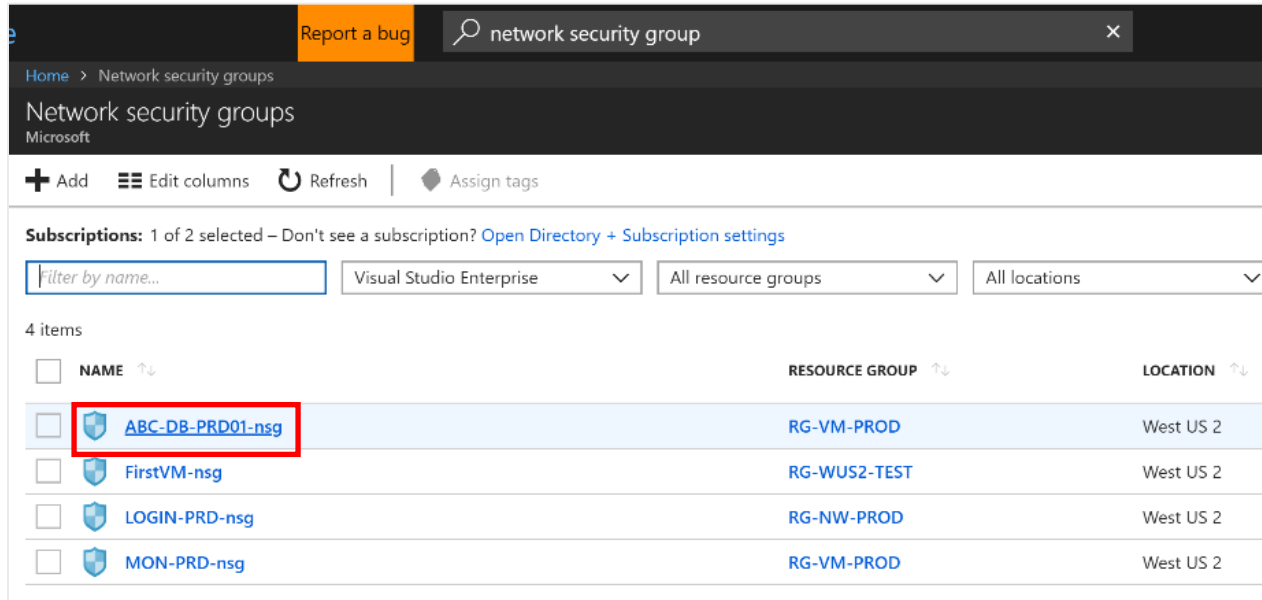
6. 보안 그룹 설정이 완료되면, 네트워크 보안 규칙 서비스 페이지로 이동합니다.



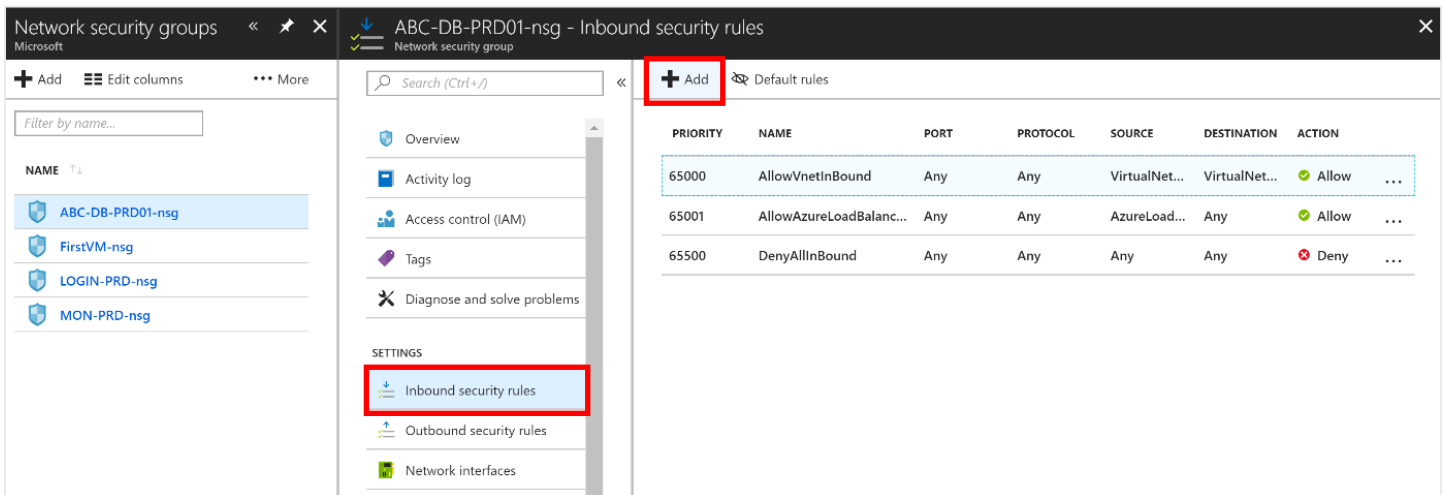
## Step 4: 네트워크 보안 그룹 구성 (인바운드 규칙 추가)

**ABC-DB-PRD01** 가상 머신이 적용 받고 있는, **ABC-DB-PRD01-nsg** 보안 규칙에 응용 프로그램 보안 그룹을 추가하여 해당 보안 그룹의 적용을 받을 수 있도록 합니다.

7. **ABC-DB-PRD01-nsg** 보안 규칙 페이지로 이동합니다.



8. 인바운드 보안 규칙 메뉴로 이동하여, +추가 버튼을 클릭하여 인바운드 보안 규칙을 추가합니다.



9. 보안 그룹을 통한 새로운 인바운드 규칙을 작성합니다. **ABC-LOGIN-ASG**의 보안 그룹을 가진 리소스만이, **ABC-DB-ASG**의 보안그룹 리소스로의 3389 접근을 허용하는 인바운드 규칙입니다. 기본적으로 같은 가상 네트워크상의 모든 리소스는 모두 통신이 가능하기 때문에, 다음 단계에서 같은 가상 네트워크 상의 통신을 거부하는 룰도 같이 추가합니다.

- Source → Application security group : ABC-LOGIN-ASG
- Source port ranges → All
- Destination → Application security group : ABC-DB-ASG
- Destination port ranges → 3389
- Priority → 1000
- Name → Allow-RDP-from-LoginASG

Add inbound security rule  
ABC-DB-PRD01-nsg

Basic

\* Source ⓘ  
Application security group

\* Source application security group ⓘ  
ABC-LOGIN-ASG

\* Source port ranges ⓘ  
\*

\* Destination ⓘ  
Application security group

\* Destination application security group ⓘ  
ABC-DB-ASG

\* Priority ⓘ  
1000 ✓

\* Name  
Allow-RDP-from-Login ✓

Description

Add

Add

10. 동일한 방법으로 **ABC-LOGIN-ASG** 를 가진 리소스 외에는 **ABC-DB-ASG** 의 3389 포트에 접근할 수 없도록, 통신을 거부하는 인바운드 규칙을 추가합니다.

- Source → Any
- Source port ranges → All
- Destination → Application security group : ABC-DB-ASG
- Destination port ranges → 3389
- Priority → 1010
- Name → Deny-RDP-except-LoginASG

Add inbound security rule  
ABC-DB-PRD01-nsg

Basic

\* Source ⓘ  
Any

\* Source port ranges ⓘ  
\*

\* Destination ⓘ  
Application security group

\* Destination application security group ⓘ  
ABC-DB-ASG

\* Destination port ranges ⓘ  
3389 ✓

\* Protocol  
Any TCP UDP

\* Action  
Allow Deny

\* Priority ⓘ  
1010 ✓

\* Name  
Deny-RDP-except-LoginASG ✓

Add

11. 이제 아래와 같이 보안 그룹과 보안 규칙 설정이 모두 완료되었습니다. **ABC-LOGIN-ASG** 보안 그룹을 가진 리소스만이 **ABC-DB-ASG** 보안 그룹의 리소스로 3389 포트에 접근할 수 있습니다. 이제 잘 적용되었는지 검증하는 실습을 해보도록 하겠습니다.

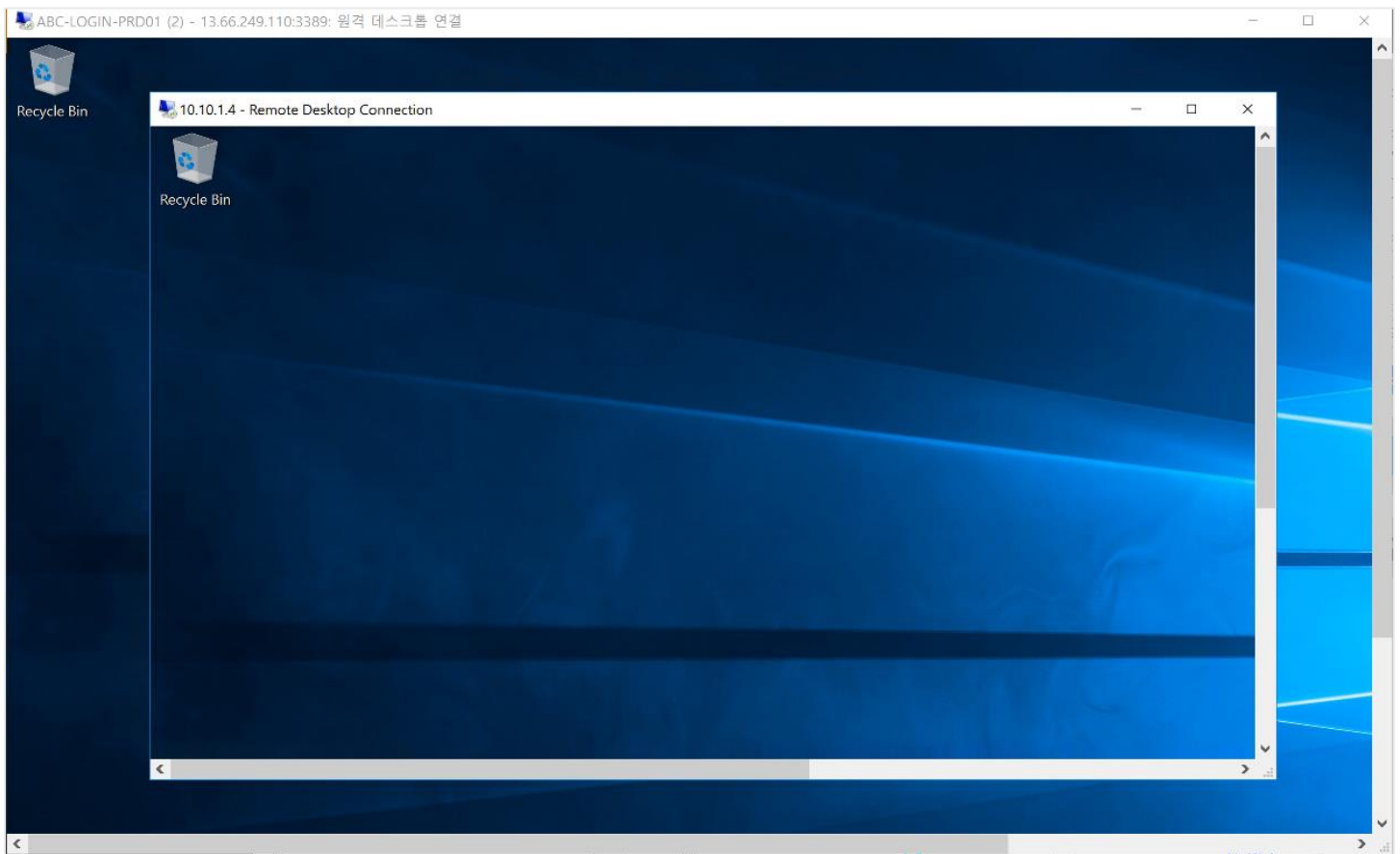
우선 순위	이름	포트	프로토콜	소스	대상 주소	작업
1000	Allow-RDP-from-Login	3389	모두	 ABC-LOGIN-ASG	 ABC-DB-ASG	 허용
1010	 Deny-RDP-except-LoginASG	3389	모두	모두	 ABC-DB-ASG	 거부
65000	AllowVnetInBound	모두	모두	VirtualNetwork	VirtualNetwork	 허용
65001	AllowAzureLoadBalancerInBound	모두	모두	AzureLoadBalancer	모두	 허용
65500	DenyAllInBound	모두	모두	모두	모두	 거부

## Step 5: 검증 시나리오

**ABC-DB-PRD01** 가상 머신이 적용 받고 있는, **ABC-DB-PRD01-nsg** 보안 규칙에 응용 프로그램 보안 그룹을 추가하여 해당 보안 그룹의 적용을 받을 수 있도록 합니다. **ABC-DB-PRD01** 가상머신은 인터넷을 통한 RDP 개방이 되어 있지 않기 때문에, 실습을 진행할때는 사설 IP 로 RDP 연결을 시도합니다. **ABC-LOGIN-PRD02** 가상머신은 보안 그룹의 적용을 받고 있지 않기 때문에 아래와 같은 결과가 나와야 합니다.

- RDP 연결 : ABC-LOGIN-PRD01 → ABC-DB-PRD01(10.10.1.4) **허용**
- RDP 연결 : ABC-LOGIN-PRD02 → ABC-DB-PRD01 **거부**

1. **ABC-LOGIN-PRD01** 가상머신에 접속하여, **ABC-DB-PRD01** 로의 RDP 접속을 시도합니다. 아래 그림과 같이 RDP 접속이 되어야 합니다.



2. **ABC-LOGIN-PRD02** 가상머신에 접속하여, **ABC-DB-PRD01** 로의 RDP 접속을 시도합니다. 실습에서 생성한 보안 그룹의 적용을 받고 있지 않기 때문에 아래 그림과 같이 RDP 접속이 되지 않아야 합니다.

