



Microsoft Cloud Workshop

Azure IaaS 101

Hands-on lab step-by-step

Lab 3

Aug 2018

Moonsun Lee (CSA)

Contents

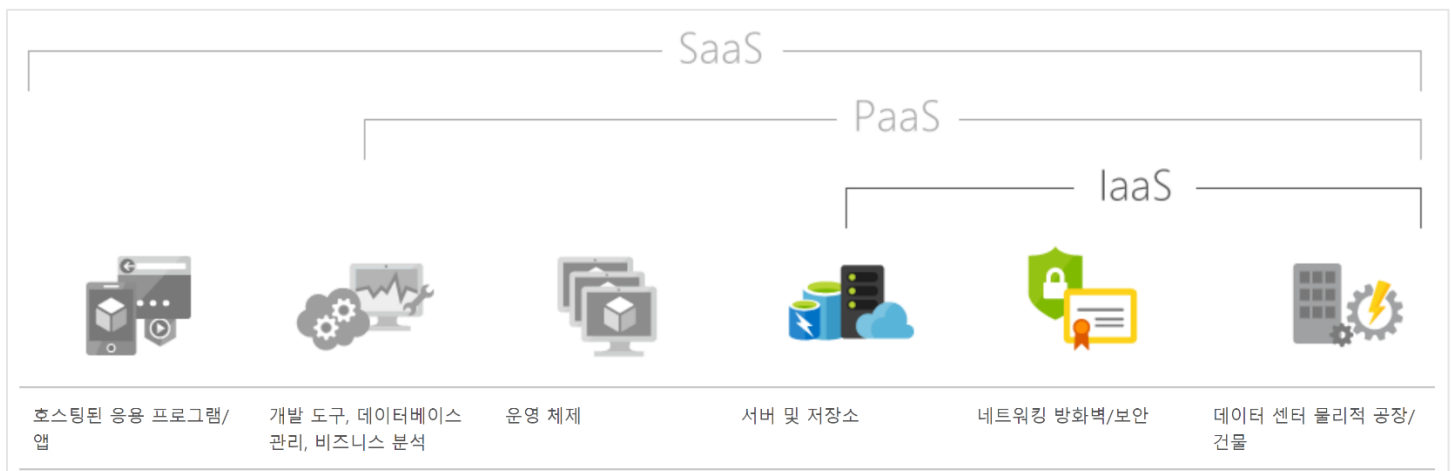
laaS 101 hands-on lab step-by-step.....	1
목표	1
Lab 구성.....	2
요구사항	2
Lab 3: Azure 인프라 디자인하기	3
Step 1: 리소스 그룹 만들기.....	3
Step 2: 가상 네트워크 만들기.....	5
Step 3: 가용성 집합 만들기.....	7
Step 4: 네트워크 보안 그룹 만들기.....	9

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.

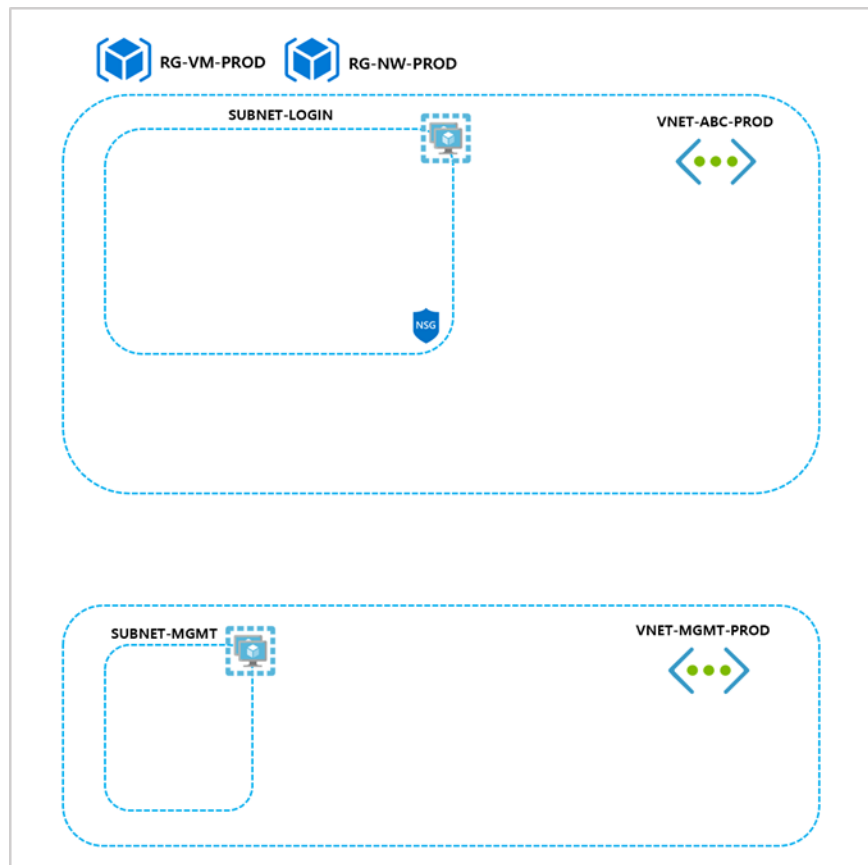
- Azure 가상머신
- Azure 가상네트워크 (서브넷 / 피어링 / 보안)
- Azure VPN 서비스
- Azure 스토리지

Lab 구성

Duration: 30 minutes

이번 실습에서는, 가상머신을 생성하기 전 "리소스 그룹 / 가상 네트워크 / 서브넷 / 가용성 집합 / 네트워크 보안 그룹" 을 미리 생성하여 실습에서 구축 할 인프라를 디자인합니다.

1. 리소스 그룹 : 가상머신 / 네트워크 리소스 관리용도 두개의 리소스 그룹 구성
2. 가상 네트워크 : 두개의 격리된 논리 네트워크 구성
3. 가용성 집합 : 가상머신가용성 집합 구성
4. 네트워크 보안 그룹 : 네트워크 필터링을 위한 보안 그룹 구성



요구사항

- Microsoft Azure subscription
- Local machine
- Lab 1 – 2 실습

Lab 3: Azure 인프라 디자인하기

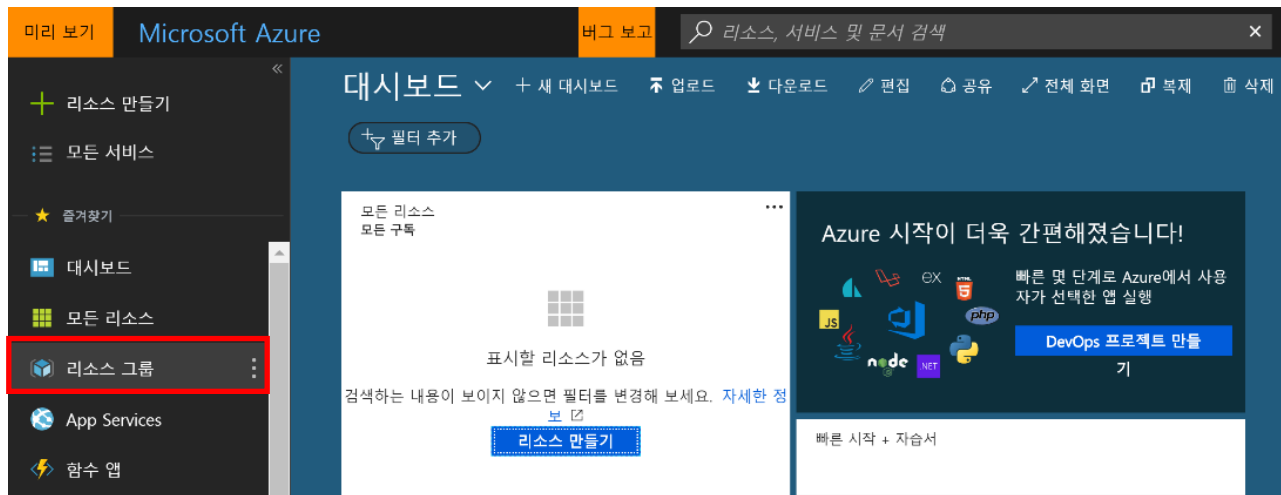
Step 1: 리소스 그룹 만들기

이번 실습에서는 가상머신 / 네트워크 리소스 관리를 위한 두개의 리소스 그룹을 생성합니다.

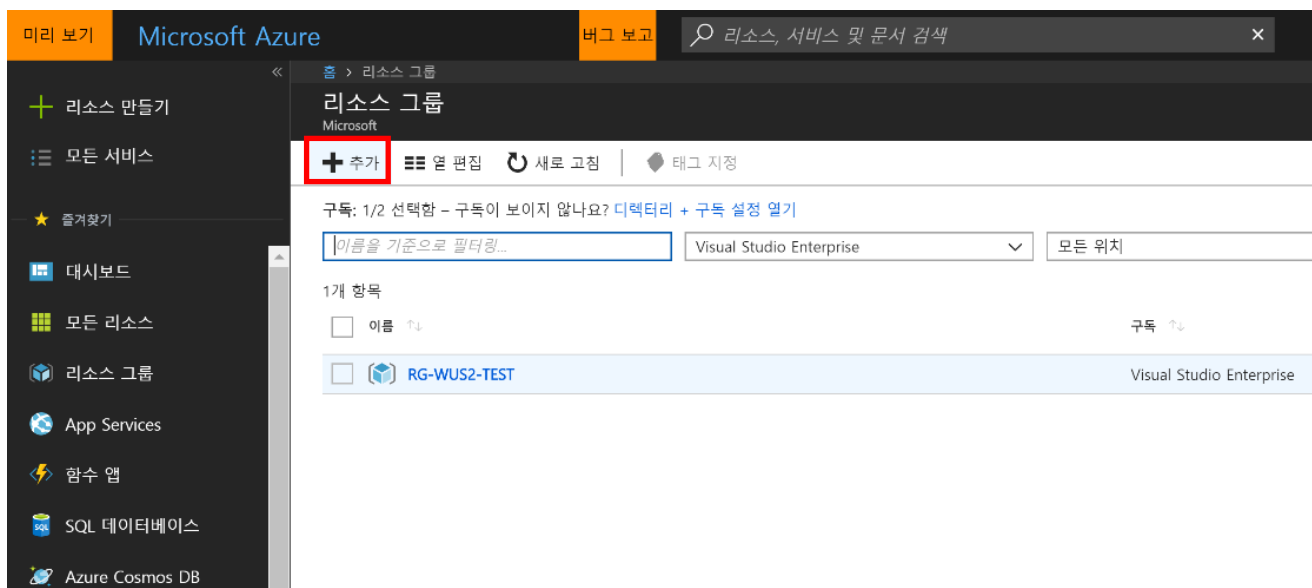
- RG-VM-PROD
- RG-NW-PROD

리소스 그룹 내 모든 리소스는 동일한 수명 주기를 공유해야 합니다. 리소스를 함께 배포, 업데이트, 삭제합니다. 예를 들어, 어플리케이션에서 데이터베이스 그룹만 다른 배포 주기가 존재하는 경우 다른 리소스 그룹에 있어야 합니다.

1. Azure 포털에서 "리소스 그룹" 페이지로 이동합니다.



2. "추가" 버튼을 클릭하여 리소스 그룹을 생성합니다.



3. 아래와 같이 리소스 그룹 정보를 입력하고, 만들기 버튼을 클릭하여 두개의 리소스 그룹을 생성합니다.

리소스 그룹 이름 : RG-VM-PROD / RG-NW-PROD

구독 : 사용할 구독 계정 선택

리소스 그룹 위치 : 미국 서부 2 (West US 2)

The image shows two side-by-side screenshots of the Microsoft Azure portal's 'Create Resource Group' form. Both forms are for the 'Visual Studio Enterprise' subscription and the '미국 서부 2' (West US 2) location. The left form is for 'RG-VM-PROD' and the right form is for 'RG-NW-PROD'. The '리소스 그룹 이름' (Resource Group Name) field is highlighted with a red box in both. The '구독' (Subscription) dropdown is set to 'Visual Studio Enterprise'. The '리소스 그룹 위치' (Resource Group Location) dropdown is set to '미국 서부 2'. The '만들기' (Create) button is highlighted with a red box at the bottom of each form.

4. 아래와 같이 리소스 그룹이 생성된 것을 확인 합니다.

리소스 그룹			
Microsoft			
<div> <div>+</div> <div>추가</div> <div>≡</div> <div>열 편집</div> <div>↺</div> <div>새로 고침</div> <div>◆</div> <div>태그 지정</div> </div>			
<div> <div>구독: 1/2 선택함 - 구독이 보이지 않나요? 디렉터리 + 구독 설정 열기</div> <div> <div>이름을 기준으로 필터링...</div> <div>Visual Studio Enterprise</div> <div>모든 위치</div> <div>No filter</div> </div> </div>			
3개 항목			
<input type="checkbox"/>	이름 ↑↓	구독 ↑↓	위치 ↑↓
<input type="checkbox"/>	RG-NW-PROD	Visual Studio Enterprise	미국 서부 2
<input type="checkbox"/>	RG-VM-PROD	Visual Studio Enterprise	미국 서부 2
<input type="checkbox"/>	RG-WUS2-TEST	Visual Studio Enterprise	미국 서부 2

Step 2: 가상 네트워크 만들기

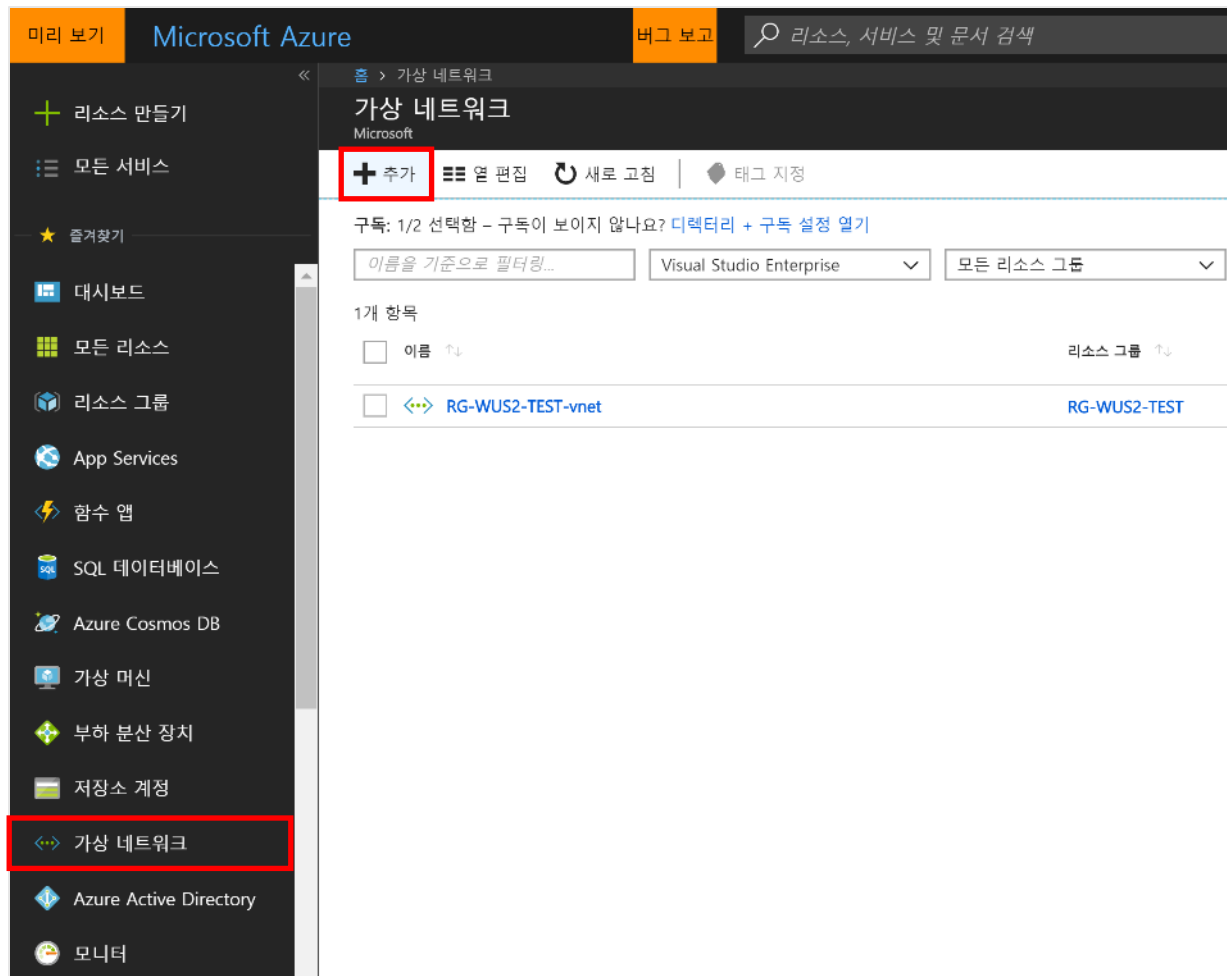
이번 실습에서는 두개의 격리된 가상 네트워크와, 해당 가상 네트워크 내 서브넷을 동시에 생성합니다.

- VNET-ABC-PROD / SUBNET-LOGIN
- VNET-ABC-MGMT / SUBNET-MGMT

Azure에서는 모든 리전에 가상 네트워크를 구현할 수 있습니다. 각 가상 네트워크는 다른 가상 네트워크와 격리됩니다.

- 공용 및 사설(RFC 1918) 주소를 사용하여 사용자가 직접 사설 IP 주소 공간을 지정합니다.
- Azure는 가상 네트워크의 리소스에 사용자가 할당한 개인 IP 주소를 할당합니다.
- 가상 네트워크를 하나 이상의 서브넷으로 분할하고 가상 네트워크 주소 공간의 일부를 각 서브넷에 할당합니다.

1. 가상 네트워크 서비스 페이지로 이동하여, "추가" 버튼을 클릭하여 생성 페이지로 이동합니다.



2. 아래와 같이 가상네트워크와 서브넷의 정보를 입력하고, 만들기 버튼을 클릭합니다.

이름	VNET-ABC-PROD	VNET-ABC-MGMT
주소 공간	10.10.0.0/16	10.20.0.0/16
리소스 그룹	기존 그룹 사용	기존 그룹 사용
	RG-NW-PROD	RG-NW-PROD
위치	미국 서부 2	미국 서부 2
서브넷 이름	SUBNET-LGOIN	SUBNET-MGMT
서브넷 주소 범위	10.10.0.0/24	10.20.0.0/24

가상 네트워크 만들기

* 이름
VNET-ABC-PROD ✓

* 주소 공간 ⓘ
10.10.0.0/16 ✓
10.10.0.0 - 10.10.255.255(65536개 주소)

* 구독
Visual Studio Enterprise ▼

* 리소스 그룹
☐ 새로 만들기 ☒ 기존 그룹 사용
RG-NW-PROD ▼

* 위치
미국 서부 2 ▼

서브넷

* 이름
SUBNET-LOGIN ✓

* 주소 범위 ⓘ
10.10.0.0/24 ✓
10.10.0.0 - 10.10.0.255(256개 주소)

DDoS 보호 ⓘ
☒ 기본 ☐ 표준

서비스 끝점 ⓘ

만들기 자동화 옵션

가상 네트워크 만들기

* 이름
VNET-ABC-MGMT ✓

* 주소 공간 ⓘ
10.20.0.0/16 ✓
10.20.0.0 - 10.20.255.255(65536개 주소)

* 구독
Visual Studio Enterprise ▼

* 리소스 그룹
☐ 새로 만들기 ☒ 기존 그룹 사용
RG-NW-PROD ▼

* 위치
미국 서부 2 ▼

서브넷

* 이름
SUBNET-MGMT ✓

* 주소 범위 ⓘ
10.20.0.0/24 ✓
10.20.0.0 - 10.20.0.255(256개 주소)

DDoS 보호 ⓘ
☒ 기본 ☐ 표준

서비스 끝점 ⓘ

만들기 자동화 옵션

3. 아래와 같이 가상 네트워크가 생성된 것을 확인 합니다.

가상 네트워크		
Microsoft		
<div> <div>+</div> 추가 <div>≡</div> 열 편집 <div>↺</div> 새로 고침 <div>◆</div> 태그 지정 </div>		
구독: 1/2 선택함 - 구독이 보이지 않나요? 디렉터리 + 구독 설정 열기		
이름을 기준으로 필터링...	Visual Studio Enterprise	모든 리소스 그룹
모든 위치		
3개 항목		
<input type="checkbox"/> 이름 ↑↓	리소스 그룹 ↑↓	위치 ↑↓
<input type="checkbox"/> <--> RG-WUS2-TEST-vnet	RG-WUS2-TEST	미국 서부 2
<input type="checkbox"/> <--> VNET-ABC-MGMT	RG-NW-PROD	미국 서부 2
<input type="checkbox"/> <--> VNET-ABC-PROD	RG-NW-PROD	미국 서부 2

Step 3: 가용성 집합 만들기

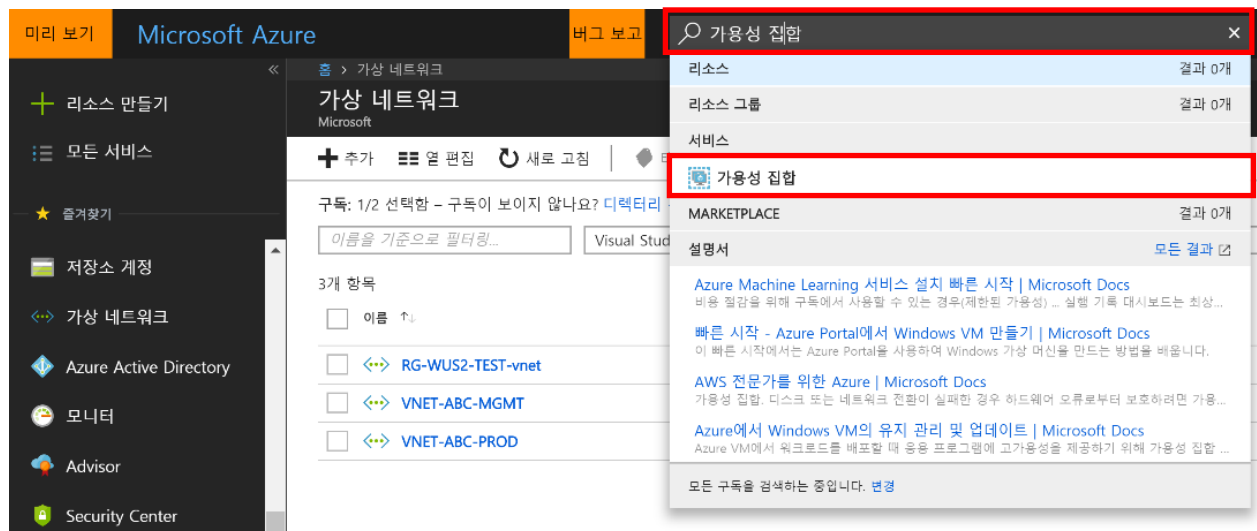
이번 실습에서는 예제로 생성되는 "Login 서버"와 "Management 서버"에 사용될 가용성 집합을 미리 생성합니다.

- AVS-LOGIN
- AVS-MGMT

가용성 집합을 사용하면 Azure 에 배포한 가상머신이 클러스터의 격리된 여러 하드웨어 노드에 분산되도록 할 수 있습니다. 이렇게 하면 Azure 내의 하드웨어 또는 소프트웨어 오류가 발생할 때 가상머신의 일부분에만 영향을 주며 전체 솔루션을 사용 가능한 운영 상태로 유지할 수 있습니다. 가용성 집합의 장애 도메인/업데이트 도메인에 대해서는 아래 페이지를 통해 더 자세히 알아볼 수 있습니다.

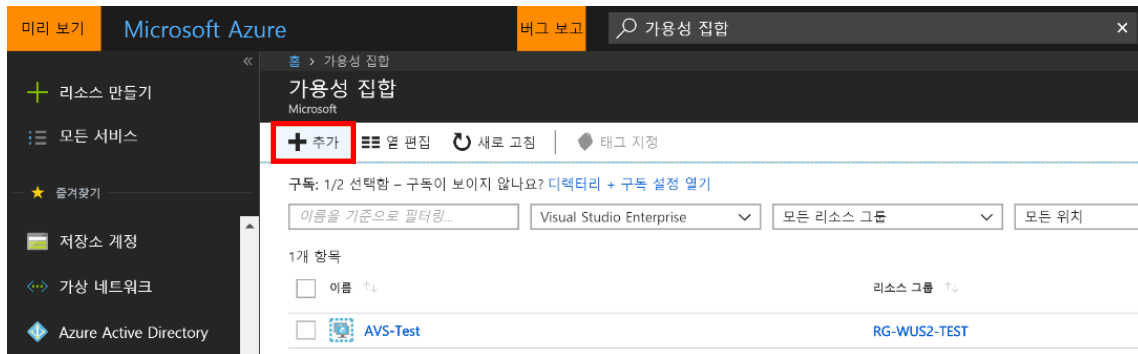
<https://blogs.technet.microsoft.com/koalra/2014/08/06/microsoft-azure-vm-availability-set-load-bala/>

1. 포털 상단의 검색 기능을 이용하여 가용성 집합 서비스 페이지로 이동합니다.



2. 가용성 집합 페이지에서 "추가" 버튼을 클릭하여, 아래와 같이 가용성 집합을 생성합니다.

- AVS-LOGIN → 장애 도메인 : 2 / 업데이트 도메인 : 5
- AVS-MGMT → 장애 도메인 : 2 / 업데이트 도메인 : 5



가용성 집합 만들기

* 이름

* 구독

* 리소스 그룹
☐ 새로 만들기 ☒ 기존 그룹 사용

* 위치

장애 도메인 ¹

업데이트 도메인 ¹

관리 디스크 사용 ¹

자동화 옵션

가용성 집합 만들기

* 이름

* 구독

* 리소스 그룹
☐ 새로 만들기 ☒ 기존 그룹 사용

* 위치

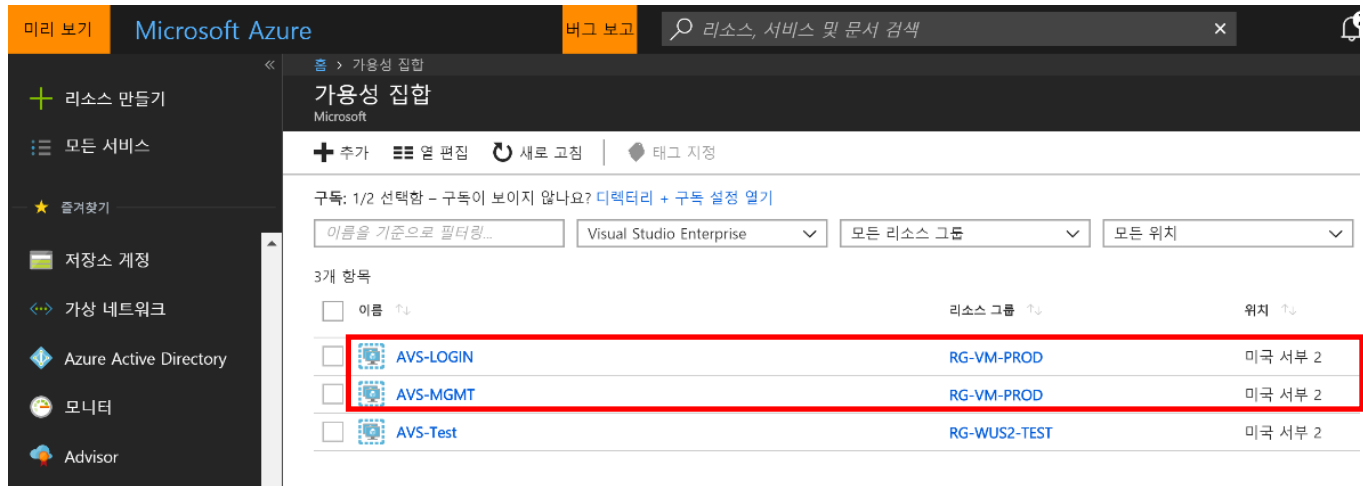
장애 도메인 ¹

업데이트 도메인 ¹

관리 디스크 사용 ¹

자동화 옵션

4. 아래와 같이 두개의 가용성 집합이 생성된 것을 확인 합니다.



Step 4: 네트워크 보안 그룹 만들기

이번 실습에서는 "Login 서버"에 적용될 네트워크 보안 그룹을 미리 생성합니다.

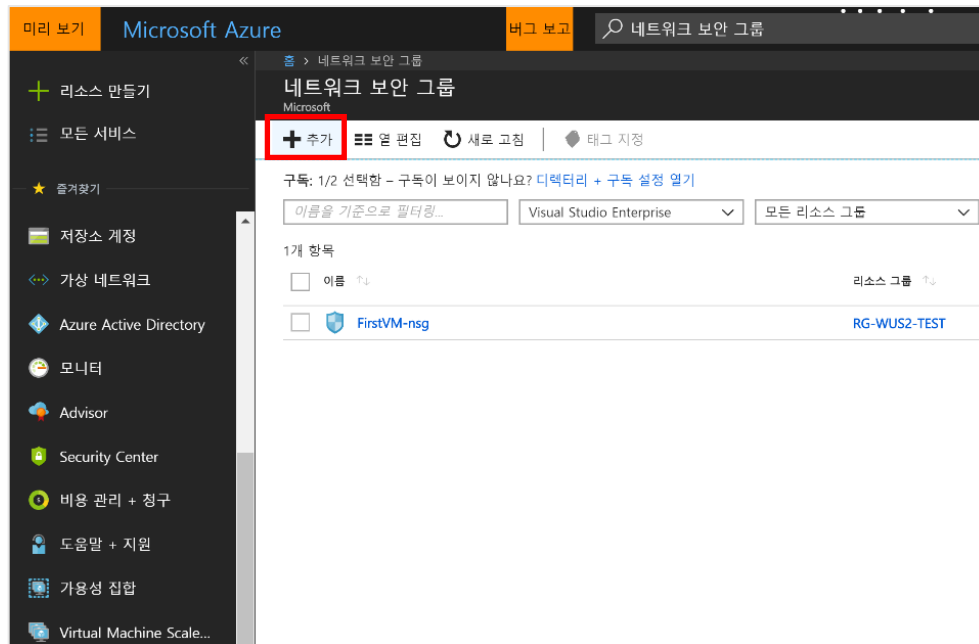
- LOGIN-PRD-nsg

네트워크 보안 그룹은, 가상 네트워크 내 Azure 리소스와 네트워크 보안 그룹이 주고받는 네트워크 트래픽을 필터링할 수 있습니다. 네트워크 보안 그룹에는 여러 종류의 Azure 리소스에서 오는 인바운드 트래픽과 이러한 리소스로 나가는 아웃바운드 네트워크 트래픽을 허용하거나 거부하는 보안 규칙이 포함됩니다. 규칙마다 원본 및 대상, 포트, 프로토콜을 지정할 수 있습니다.

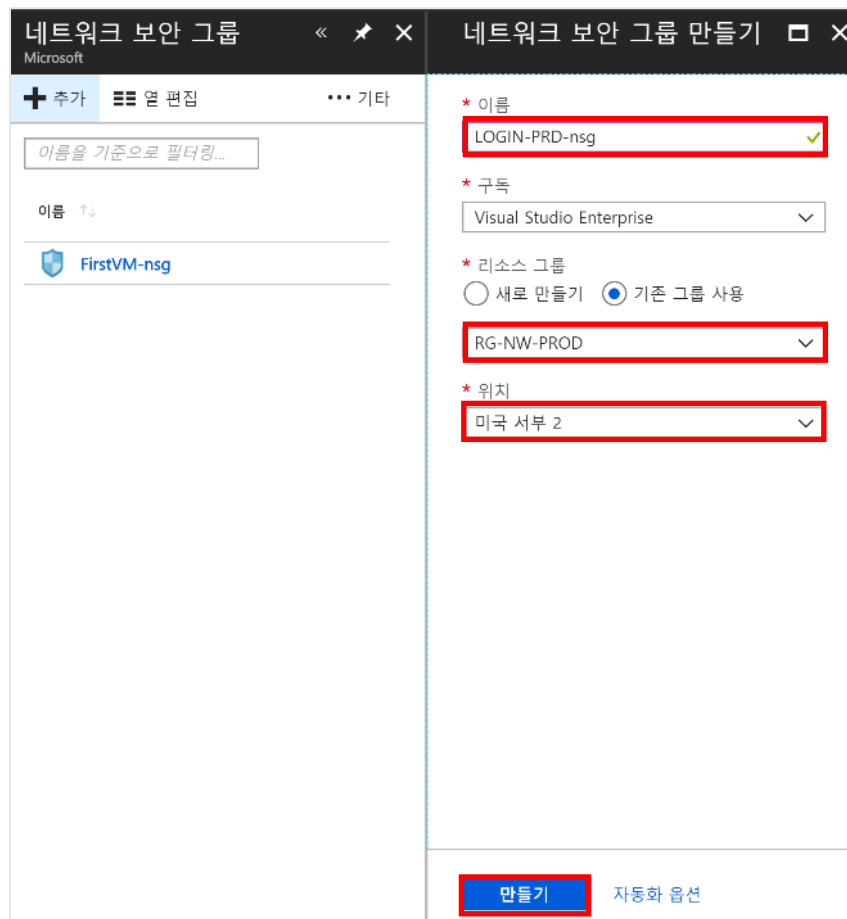
1. 포털 상단의 검색 기능을 이용하여 네트워크 보안 그룹 페이지로 이동합니다.



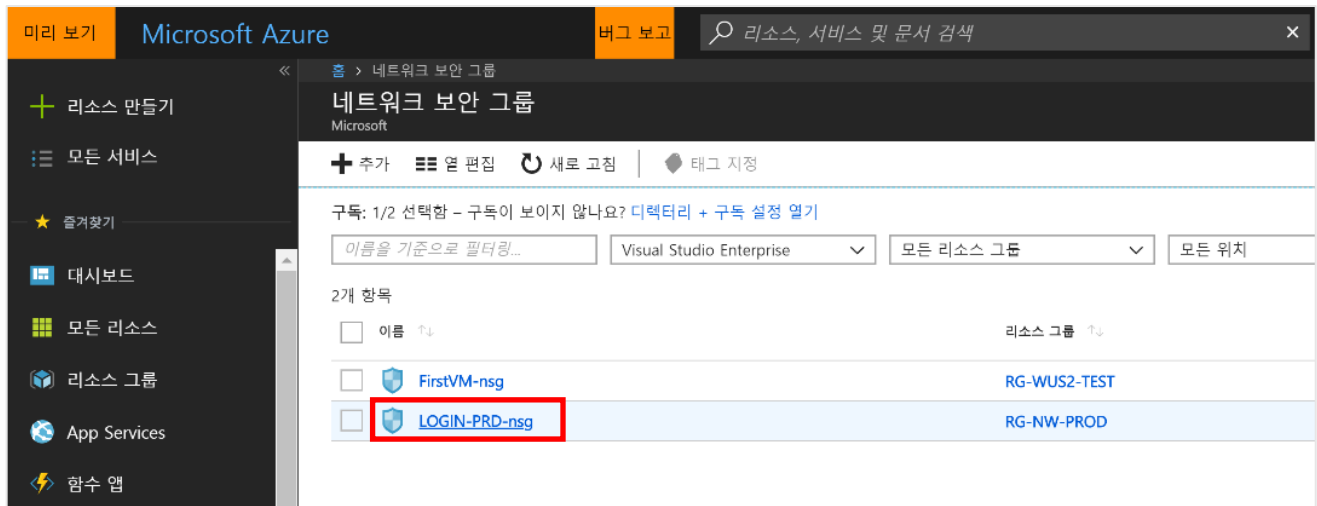
2. 추가 버튼을 클릭하여, "Login 서버"에 적용될 네트워크 보안 그룹을 생성합니다.



3. 아래와 같이 이름에 "LOGIN-PRD-nsg"를 입력한 뒤 네트워크 리소스 그룹을 선택하고, 만들기 버튼을 클릭합니다.

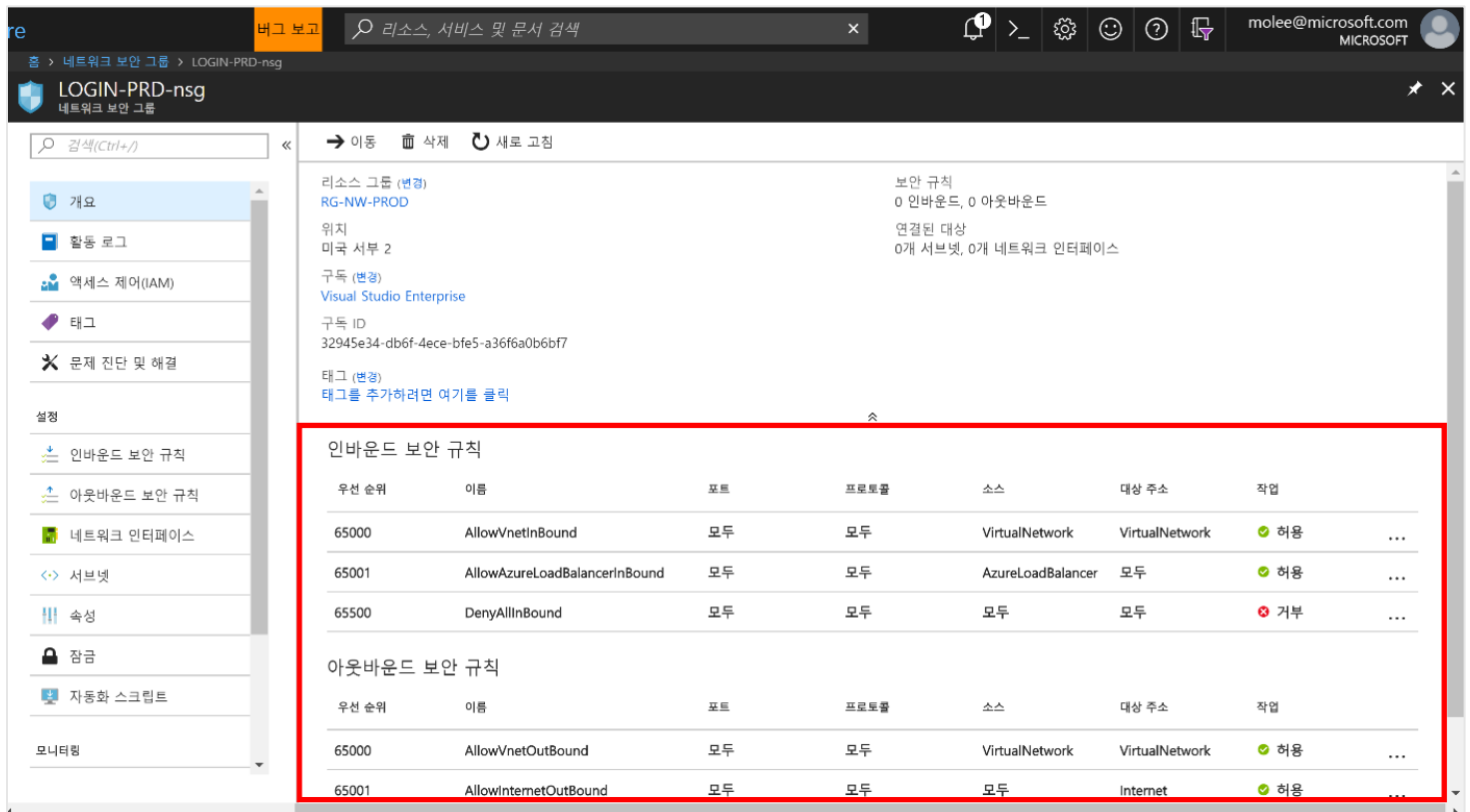


4. 보안 그룹이 생성되면, 생성된 보안 그룹을 클릭하여 상세 페이지로 이동합니다.

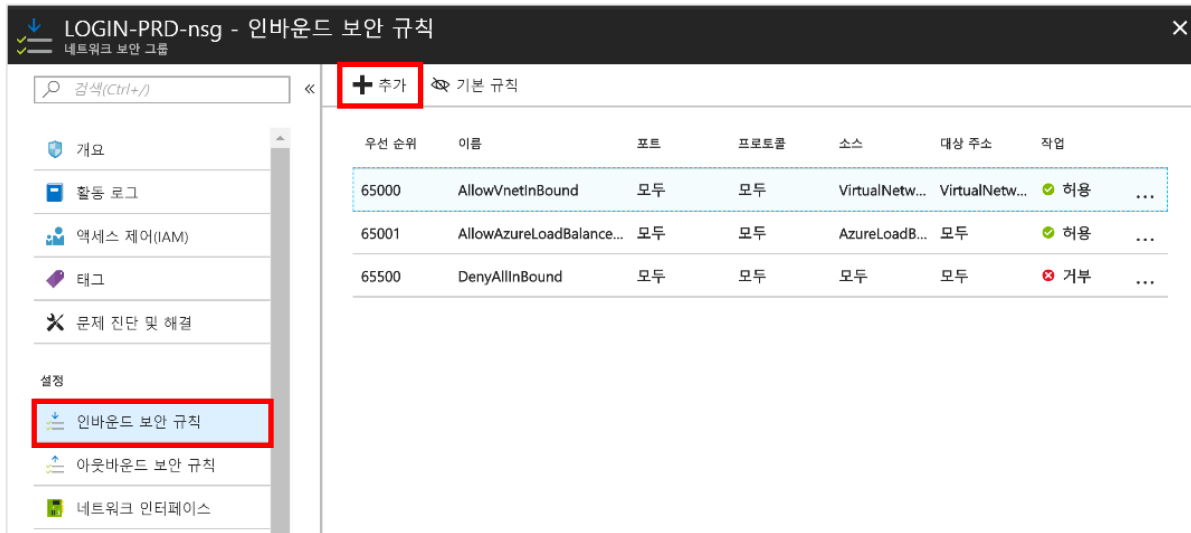


5. 보안 그룹 상세 페이지에서, 해당 보안 그룹의 인바운드 및 아웃바운드 정책을 설정할 수 있습니다. 개요 페이지에서 볼 수 있듯이 아래와 같은 Azure의 기본 보안 규칙이 자동적으로 생성됩니다.

(참고 : <https://docs.microsoft.com/ko-kr/azure/virtual-network/security-overview#default-security-rules>)



- 인바운드 보안 규칙을 클릭하여 인바운드 보안 규칙 탭으로 이동합니다. 이곳에서 해당 보안 그룹의 인바운드 정책을 설정할 수 있습니다. 3389 포트를 오픈하여, 해당 보안 그룹이 적용될 Login 서버에서 RDP 를 허용하도록 합니다.
추가 버튼을 클릭하여 인바운드 보안규칙을 생성한 보안그룹에 추가합니다.



cf. Azure 네트워크 보안 규칙 속성

소스 / 대상주소	모두, 개별 IP 주소, CIDR 블록(예: 10.0.0.0/24), 서비스 태그 또는 응용 프로그램 보안 그룹.
프로토콜	TCP, UDP 또는 TCP, UDP 및 ICMP 를 포함하는 모두이며, ICMP 를 단독으로 지정할 수 없으므로 ICMP 가 필요한 경우 다른 프로토콜과 함께 사용.
포트범위	개별 포트나 포트의 범위를 지정. 예를 들어 80 또는 10000-10005 과 같이 지정.
작업	허용 또는 거부.
우선순위	100~4096 사이의 숫자이며, 낮은 번호의 우선 순위가 더 높기 때문에 보안규칙은 낮은 번호가 높은 번호보다 먼저 처리되는 우선 순위 순서로 처리. 트래픽이 규칙과 일치하면 처리가 중지. 따라서 우선 순위가 높은 규칙과 동일한 특성을 가진 우선 순위가 낮은 규칙(높은 번호)은 처리되지 않음.

네트워크 보안 그룹 보안 규칙은 5 튜플 정보(원본, 원본 포트, 대상, 대상 포트 및 프로토콜)를 사용하는 우선 순위를 통해 평가되어 트래픽을 허용하거나 거부합니다. 기존 연결에 대한 플로우 레코드가 만들어집니다. 네트워크는 플로우 레코드의 연결 상태에 따라 허용 또는 거부됩니다. 플로우 레코드는 네트워크 보안 그룹의 상태 저장을 허용합니다. 예를 들어 포트 80 을 통해 모든 주소에 대한 아웃바운드 보안 규칙을 지정하는 경우 아웃바운드 트래픽에 대한 응답에 인바운드 보안 규칙을 지정하지 않아도 됩니다. 통신이 외부에서 시작된 경우 인바운드 보안 규칙을 지정하기만 하면 됩니다. 반대의 경우도 마찬가지입니다. 포트를 통해 인바운드 트래픽이 허용되는 경우 포트를 통해 트래픽에 응답하도록 아웃바운드 보안 규칙을 지정하지 않아도 됩니다. 흐름을 사용하는 보안 규칙을 제거해도 기존 연결이 중단되지 않을 수 있습니다. 연결이 중단되고 몇 분 이상 어느 방향으로든 트래픽이 흐르지 않으면 플로우 레코드는 중단됩니다.

7. 해당 보안 그룹이 적용될 "Login 서버"에서 RDP 를 허용하는 보안 규칙을 생성합니다. 아래 설정정보를 입력하고 만들기 버튼을 클릭합니다.

- 소스 및 대상주소 → Any
- 원본 포트 범위 → * (All)
- 프로토콜 → TCP
- 작업 → 허용
- 우선순위 → 300
- 이름 : RDP (Allow_RDP_from_Internet)

인바운드 보안 규칙 추가
LOGIN-PRD-nsg

기본

* 소스 ⓘ
Any

* 원본 포트 범위 ⓘ
*

* 대상 주소 ⓘ
Any

* 대상 포트 범위 ⓘ
3389 ✓

* 프로토콜
Any TCP UDP

* 작업
허용 거부

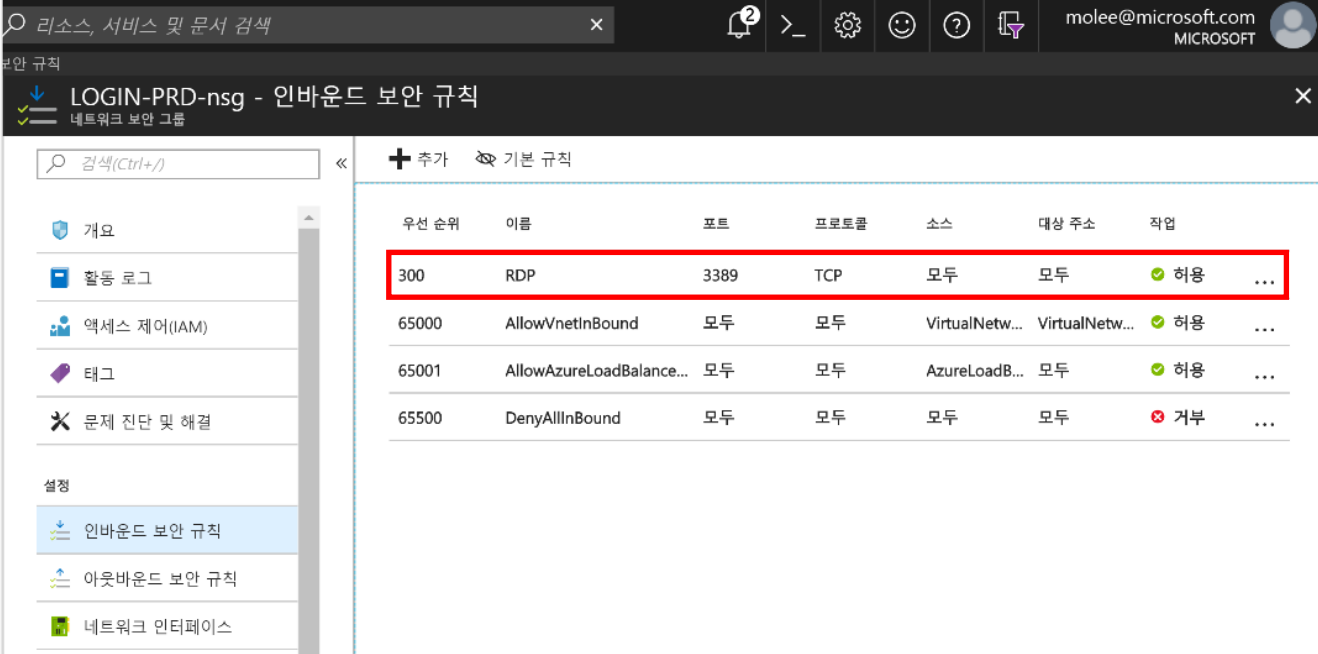
* 우선 순위 ⓘ
300 ✓

* 이름
RDP ✓

설명

추가

8. 아래와 같이 RDP(포트:3389)에 대한 인바운드 보안 규칙이 LOGIN-PRD-nsg 에 생성되어 적용된 것을 확인할 수 있습니다. 이와 같은 규칙을 이용하여, 어플리케이션에 대한 포트를 개방하고 소스/대상을 지정하여 사내 보안정책을 손쉽게 강력하게 적용할 수 있습니다.



The screenshot displays the Azure portal interface for configuring inbound security rules for the 'LOGIN-PRD-nsg' network security group. The left sidebar shows navigation options like '개요' (Overview), '활동 로그' (Activity Log), '액세스 제어(IAM)' (Access Control (IAM)), '태그' (Tags), '문제 진단 및 해결' (Troubleshooting and Resolution), and '설정' (Settings). Under '설정', '인바운드 보안 규칙' (Inbound Security Rules) is selected. The main pane shows a table of security rules with columns: '우선 순위' (Priority), '이름' (Name), '포트' (Port), '프로토콜' (Protocol), '소스' (Source), '대상 주소' (Destination Address), and '작업' (Actions). The first rule, 'RDP', is highlighted with a red border. It has a priority of 300, allows TCP traffic on port 3389 from all sources to all destinations.

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