



Azure Fundamentals

- IaaS

Focus on Cloud

Microsoft Azure Consulting Expert Group

Cloocus
Beyond the Cloud

Gold
Microsoft
Partner
 Microsoft



Module 1.

Microsoft Azure 시작하기

Cloud Computing

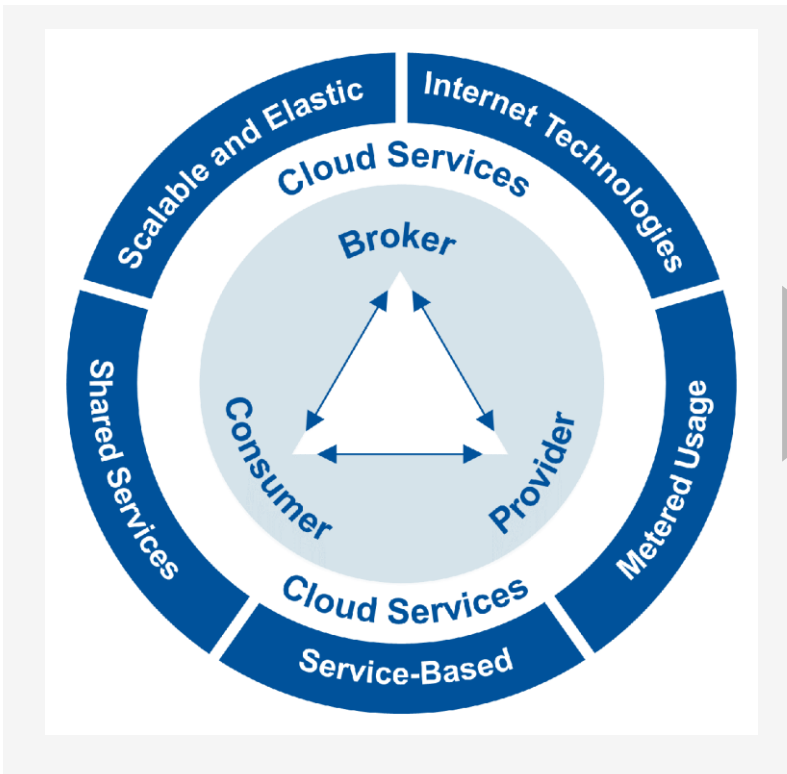
클라우드 컴퓨팅은 "인터넷 기술을 활용하여 다수의 고객들에게 높은 확장성을 가진 자원들을 서비스로 제공하는 컴퓨팅의 한 형태"로 공유 자원, 셀프 서비스, 유연성, 그리고 사용량 기반 이라는 특성을 가지고 있습니다

Cloud Computing 정의

Gartner

인터넷 기술을 활용하여 다수의 고객들에게 높은 확장성을 가진 자원들을 서비스로 제공하는 컴퓨팅의 한 형태

Cloud Computing 개요



Source: Gartner (April 2016)

Cloud Computing 특성



네트워크 접근
공유 자원

- 데이터 안전을 위한 노력
- 이용자가 데이터를 소유하고 제어



사용자 중심의
셀프 서비스

- 단일 콘솔에서 빌드, 관리 및 모니터링
- 프로세스 자동화를 통한 관리 간소화



신속한
유연성

- 몇 분 안에 1,000개의 인스턴스 배포
- 수요에 맞춰 자동 크기 조정 및 비용 절감



계량 가능한
사용량 기반

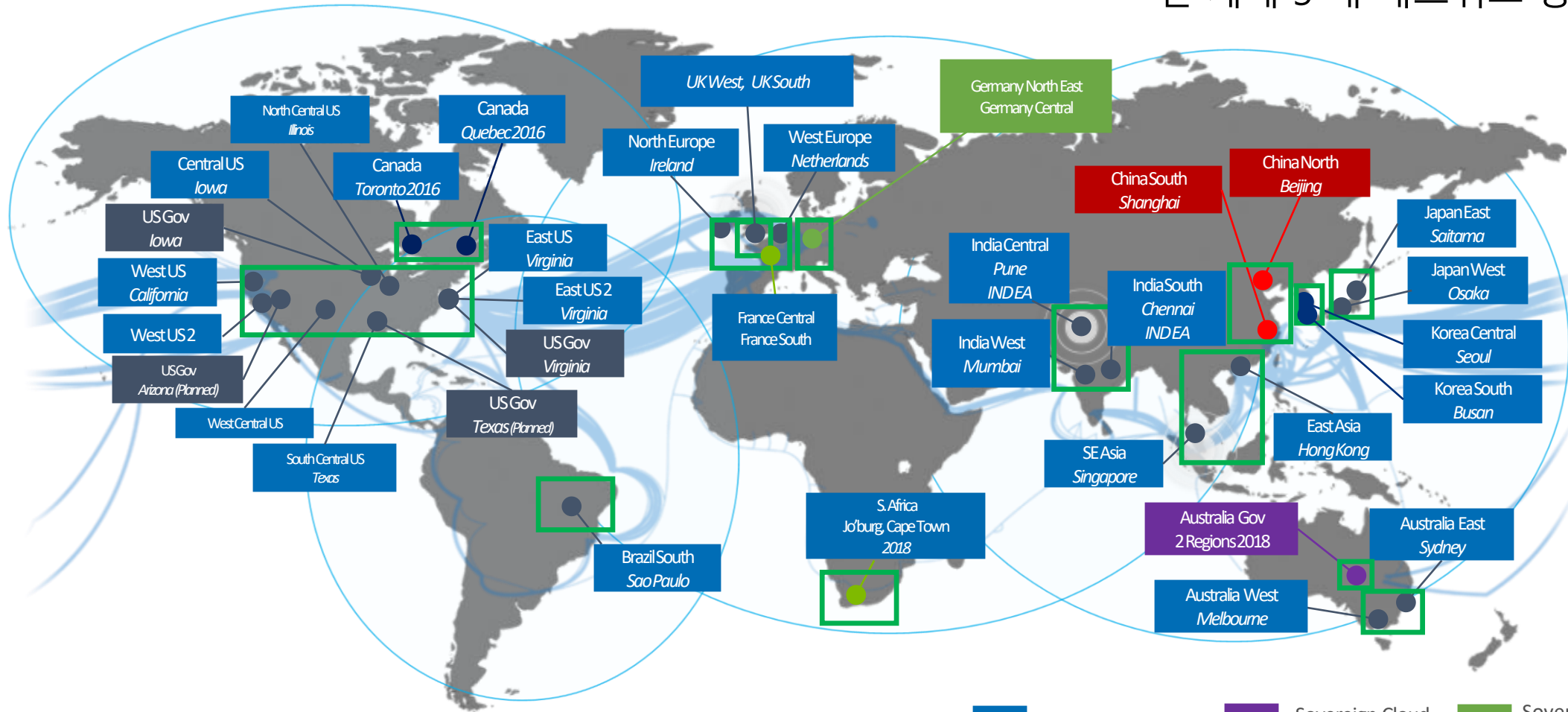
- 분당 요금으로 비용 절약

Azure Global Footprint

54 regions worldwide

140 available in 140 countries

전 세계 3 대 네트워크 중 하나

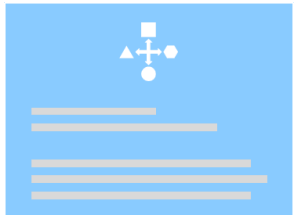


<https://azure.microsoft.com/en-us/global-infrastructure/regions/>

- Public Azure
- Sovereign Cloud Australia (CDC)
- Sovereign Cloud Germany (T-Systems)
- Planned
- US Gov Cloud
- Sovereign Cloud China (21 Vianet)

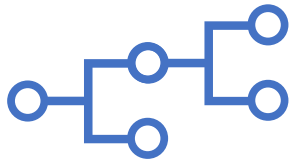
Azure 생태계

응용 프로그램



- Windows | Linux
- Java, PHP, .NET, ...
- IaaS
- PaaS
- 컨테이너

운영



- 템플릿
- PowerShell, CLI
- Puppet, Chef, DSC
- 메트릭
- 진단

도구



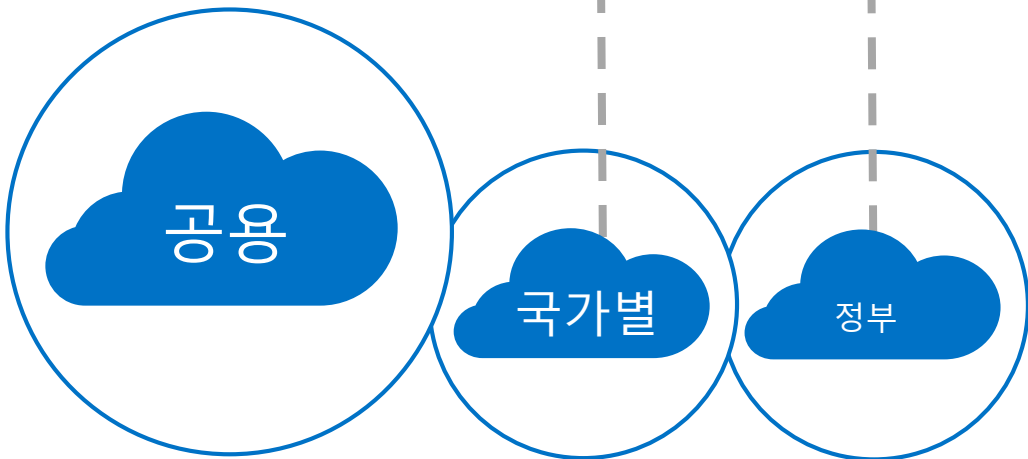
- Visual Studio
- Eclipse
- 기타

경험



- 포털
- 갤러리
- RBAC
- GitHub

Azure 생태계



서비스
공급자

기업



Microsoft Azure

Microsoft Azure Stack

Azure Service Map

플랫폼 서비스

보안 & 관리

- 포털
- Active Directory
- 다단계 인증
- 자동화
- 키 자격 증명 모음
- 스토어 / 마켓플레이스
- VM 이미지 갤러리 & VM Depot

계산

- 클라우드 서비스
- 서비스 팩브릭
- 배치
- Remote App

웹 및 모바일

- 웹 앱
- API 앱
- API 관리
- 모바일 앱
- 로직 앱
- 알림 허브

개발자 서비스

- Visual Studio
- Azure SDK
- 팀 프로젝트
- Application Insights

하이브리드 운영

- Azure AD Connect Health
- AD 권한 있는 ID 관리
- 백업
- Operational Insights
- 가져오기/내보내기
- Site Recovery
- StorSimple

통합

- 저장소 큐
- BizTalk 서비스
- 하이브리드 연결
- 서비스 버스

분석 & IoT

- HDInsight
- 머신 러닝
- 데이터 팩터리
- 이벤트 허브
- 스트림 분석
- Mobile Engagement

데이터

- SQL 데이터베이스
- SQL 데이터 웨어하우스
- Redis Cache
- 검색
- Cosmos DB
- 테이블

미디어 & CDN

- 미디어 서비스
- 콘텐츠 배달 네트워크(CDN)

인프라 서비스

계산

- 가상 컴퓨터
- 컨테이너

저장소

- BLOB 저장소
- 파일
- 프리미엄 저장소

네트워킹

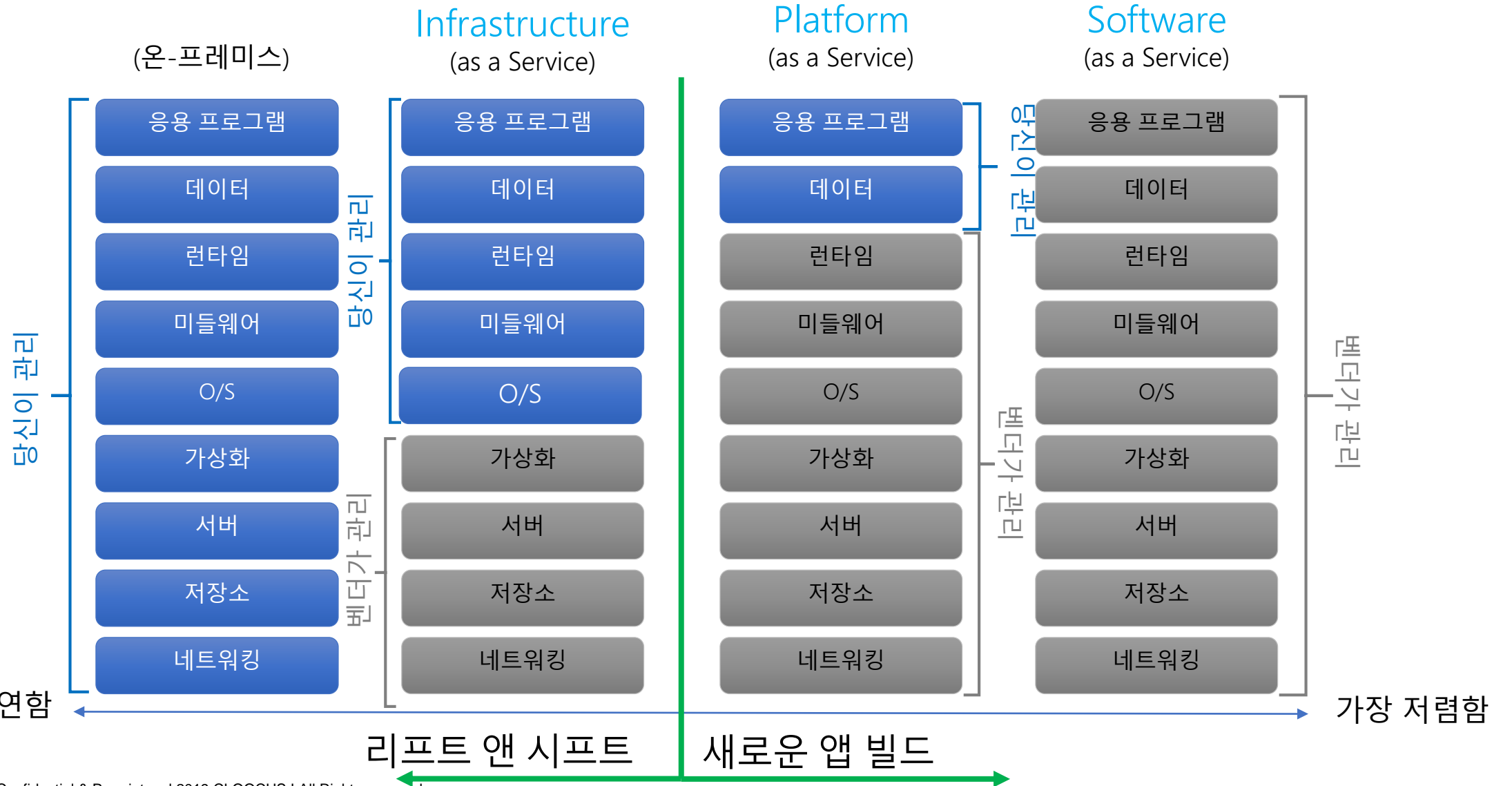
- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

데이터센터 인프라



Shared Responsibility

Microsoft Azure



구독, 계정

Account & Subscription

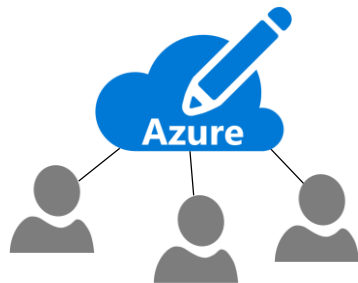
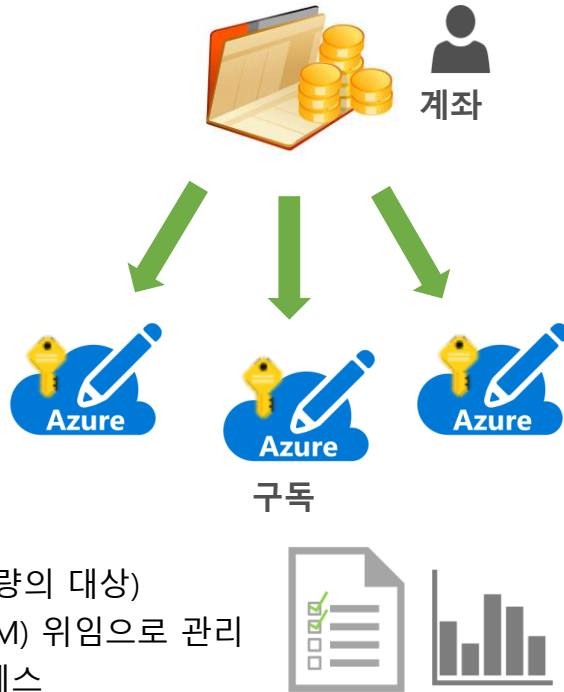
계정과 구독

✓ 계정(Account)

- 과금 및 보고 기능
- 구독의 컨테이너
- 계정 관리자가 관리

✓ 구독(Subscription)

- 과금 및 관리의 경계
- 리소스의 컨테이너(할당량의 대상)
- 서비스 관리자, RBAC(IAM) 위임으로 관리
- Azure Portal을 통해 액세스



Identity

✓ 조직 계정(Work or School account)

- 구독을 Azure Active Directory나 Office 365 테넌트와 연결 (실제로 둘 다 동일함)
- 기존 Identity로 Azure에 액세스 관리



✓ Microsoft 계정

- 기존의 조직 계정 이메일과 연결되어 있지 않고 만든 계정
- Outlook.com / Hotmail.com 등



구독, 계정

Subscription – Service limits

구독별 서비스 할당량 제한

Azure 구독은 할당량과 서비스 제한을 가지고 있음. 서비스 제한에 도달하면 새로운 구독을 만들어야 함.

제한 설정을 아는 것은 구독 사용량과 리소스 관리를 계획하는데 있어 중요함

구독 - 사용량 및 할당량

각 Microsoft Azure 리소스를 자체 할당량까지 사용할 수 있습니다. 각 구독에 별도의 할당량이 있으며 사용 현황이 구독별로 추적됩니다. 할당량 한도에 도달하면 도움말 + 지원을 통해 할당량 증가를 요청할 수 있습니다. [자세한 정보](#)

모든 서비스 할당량 | 모든 공급자 | 모든 위치 | 사용량을 포함하는 항목만 표시

할당량	공급자	위치	사용량	한도
Network Watchers	Microsoft.Network	동아시아	100%	1/1
Network Watchers	Microsoft.Network	한국 중부	100%	1/1
지역별 총 vCPU	Microsoft.Compute	한국 중부	85%	17/20
표준 Dsv2 제품군 vCPUs	Microsoft.Compute	한국 중부	35%	7/20
표준 Dsv3 제품군 vCPUs	Microsoft.Compute	한국 중부	30%	6/20
표준 BS 제품군 vCPUs	Microsoft.Compute	한국 중부	20%	4/20
지역별 총 vCPU	Microsoft.Compute	동아시아	10%	2/20
표준 Dsv3 제품군 vCPUs	Microsoft.Compute	동아시아	10%	2/20
Public IP Addresses	Microsoft.Network	한국 중부	1%	6/1000
Storage Accounts	Microsoft.Storage	아시아 남동부	0%	1/250
Virtual Networks	Microsoft.Network	한국 중부	0%	3/1000
Network Security Groups	Microsoft.Network	한국 중부	0%	7/5000
Public IP Addresses	Microsoft.Network	동아시아	0%	1/1000
Static Public IP Addresses	Microsoft.Network	동아시아	0%	1/1000
Static Public IP Addresses	Microsoft.Network	한국 중부	0%	1/1000
Virtual Networks	Microsoft.Network	동아시아	0%	1/1000
가용성 집합	Microsoft.Compute	한국 중부	0%	1/2000
가상 머신	Microsoft.Compute	한국 중부	0%	9/25000
Network Security Groups	Microsoft.Network	동아시아	0%	1/5000

<https://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/>



Module 2.

Microsoft Azure 관리 도구

Azure Portal

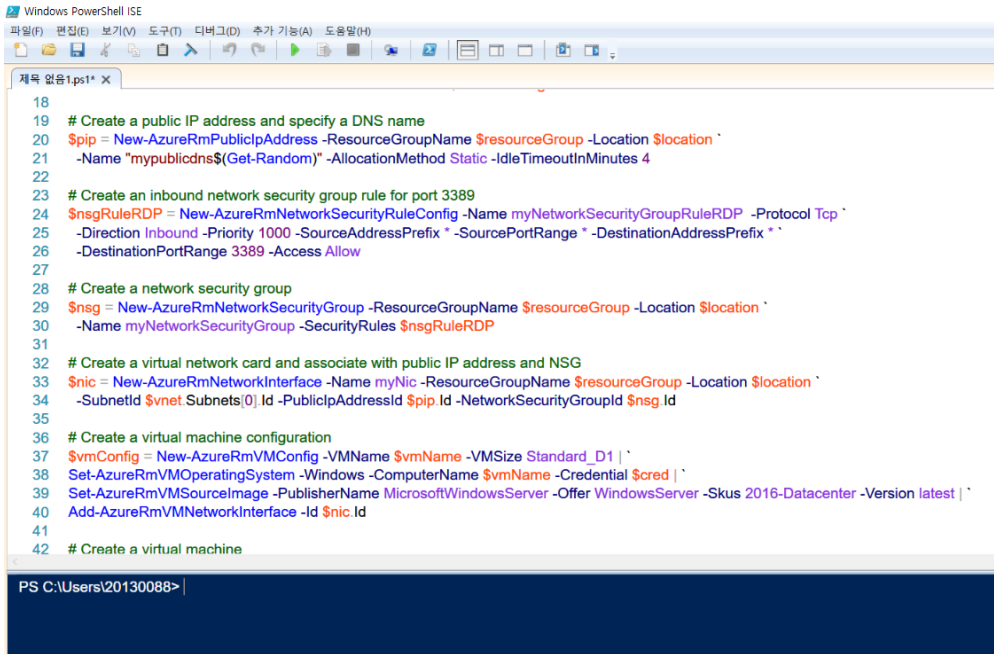
Azure Portal (portal.azure.com)



[Azure Mobile App]

Azure Command Tools

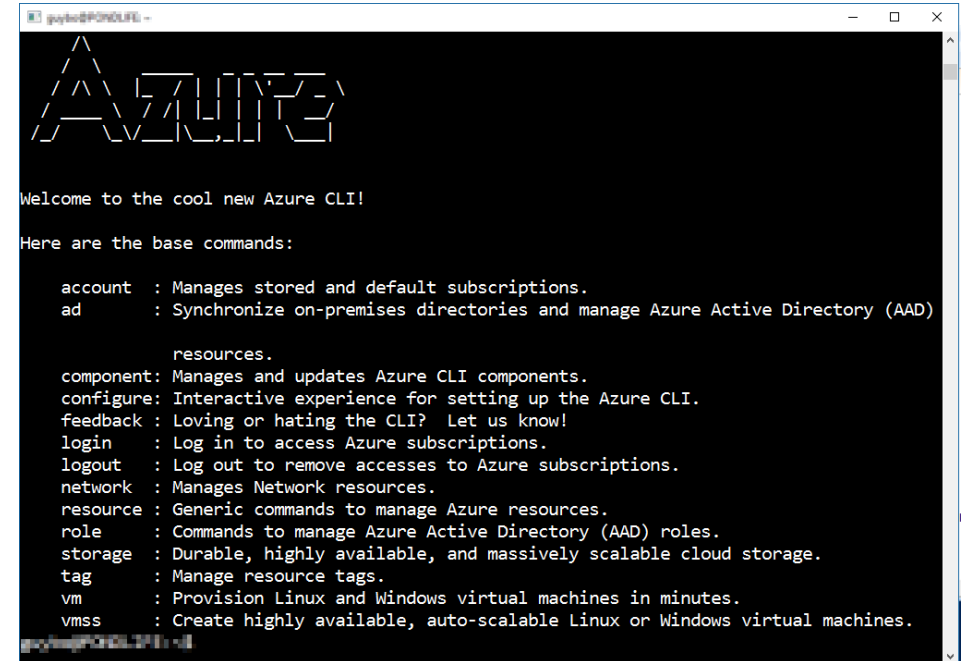
PowerShell



```
18
19 # Create a public IP address and specify a DNS name
20 $pip = New-AzureRmPublicIpAddress -ResourceGroupName $resourceGroup -Location $location `
21     -Name "mypublicdns$(Get-Random)" -AllocationMethod Static -IdleTimeoutInMinutes 4
22
23 # Create an inbound network security group rule for port 3389
24 $nsgRuleRDP = New-AzureRmNetworkSecurityRuleConfig -Name myNetworkSecurityGroupRuleRDP -Protocol Tcp `
25     -Direction Inbound -Priority 1000 -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix * `
26     -DestinationPortRange 3389 -Access Allow
27
28 # Create a network security group
29 $nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $resourceGroup -Location $location `
30     -Name myNetworkSecurityGroup -SecurityRules $nsgRuleRDP
31
32 # Create a virtual network card and associate with public IP address and NSG
33 $nic = New-AzureRmNetworkInterface -Name myNic -ResourceGroupName $resourceGroup -Location $location `
34     -SubnetId $vnet.Subnets[0].Id -PublicIpAddressId $pip.Id -NetworkSecurityGroupId $nsg.Id
35
36 # Create a virtual machine configuration
37 $vmConfig = New-AzureRmVMConfig -VMName $vmName -VMSize Standard_D1 | `
38     Set-AzureRmVMOperatingSystem -Windows -ComputerName $vmName -Credential $cred | `
39     Set-AzureRmVMSourceImage -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-Datacenter -Version latest | `
40     Add-AzureRmVMNetworkInterface -Id $nic.Id
41
42 # Create a virtual machine
```

- AzureRM
- AZ module

CLI 2.0



```
guy@PS C:\Users\guy> az
Welcome to the cool new Azure CLI!

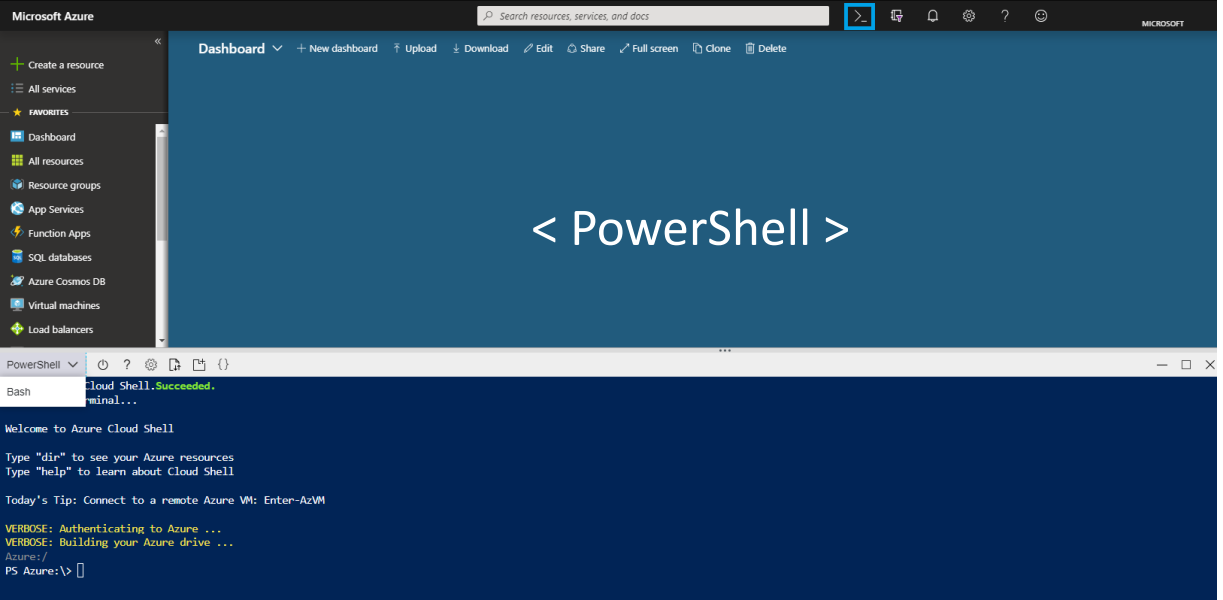
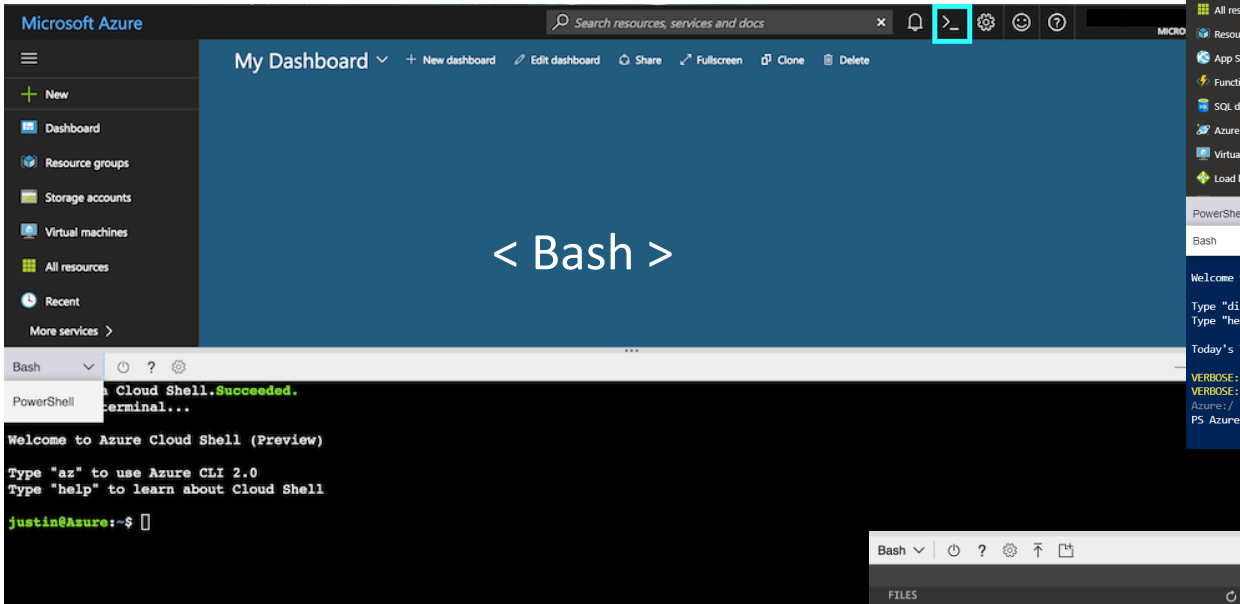
Here are the base commands:

account : Manages stored and default subscriptions.
ad       : Synchronize on-premises directories and manage Azure Active Directory (AAD)
          resources.
component: Manages and updates Azure CLI components.
configure: Interactive experience for setting up the Azure CLI.
feedback : Loving or hating the CLI? Let us know!
login    : Log in to access Azure subscriptions.
logout   : Log out to remove accesses to Azure subscriptions.
network  : Manages Network resources.
resource : Generic commands to manage Azure resources.
role     : Commands to manage Azure Active Directory (AAD) roles.
storage  : Durable, highly available, and massively scalable cloud storage.
tag      : Manage resource tags.
vm       : Provision Linux and Windows virtual machines in minutes.
vmss    : Create highly available, auto-scalable Linux or Windows virtual machines.
```

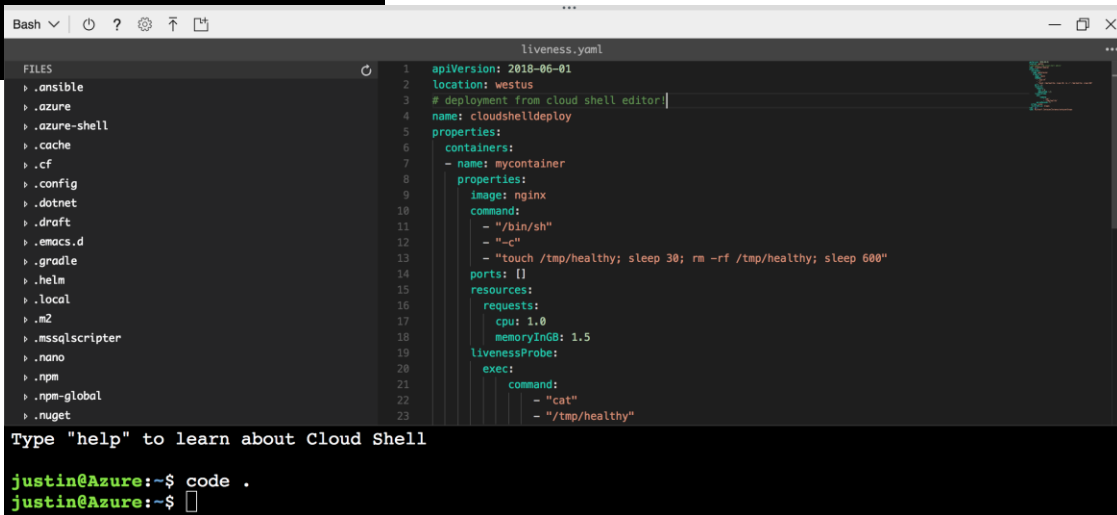
- 최신 버전: 2.0.64
- az 명령
- 파이썬 기반
- Windows(PowerShell, WSL), Linux, macOS 에서 설치 가능
- 리눅스 셸 스크립팅 도구와 통합

Azure Command Tools

Cloud Shell




- 브라우저에서 액세스할 수 있는 대화형 셸
- Bash 또는 PowerShell 중 하나를 선택
- 계정 액세스를 자동으로 인증
- 20분 후 자동으로 종료
- Monaco 편집기 제공
- Mobile App에서 지원





Azure Command Tools

도구 & 확장


 **Visual Studio**
Windows용 다운로드
Mac용 다운로드


 **Java 도구**
Maven 플러그 인
IntelliJ 및 Eclipse
Visual Studio Code


 **Storage Explorer**
시작
Linux용 다운로드
Mac용 다운로드
Windows용 다운로드


 **Visual Studio Code**
App Service
Azure Functions
Storage
Cosmos DB


 **Python 도구**
Visual Studio
Visual Studio Code

 **Service Fabric SDK 및 Tools**
Windows용 다운로드
Linux용 다운로드
Mac OS X 다운로드
Service Fabric CLI 다운로드


 **Docker**
Visual Studio Tools for Docker
Visual Studio용 다운로드
Visual Studio Code용 다운로드
Azure DevOps용 다운로드


 **Azure 리소스 관리자**
Visual Studio
Visual Studio Code
샘플 템플릿
참조


 **SQL 도구**
Azure Data Studio ^{PREVIEW}
SSMS(SQL Server Management Studio)
SSDT(SQL Server Data Tools)
모든 SQL 도구 참조


 **Azure Dev 공간**
시작
.NET Core 및 VS Code용 다운로드
.NET Core 및 Visual Studio용 다운로드
Node.js용 다운로드


언어 & 프레임워크


 **.NET 개발자용 Azure**
시작
API 참조

 **Java 개발자용 Azure**
시작
API 참조

 **Python 개발자용 Azure**
시작
API 참조

 **Go 개발자용 Azure**
시작
API 참조

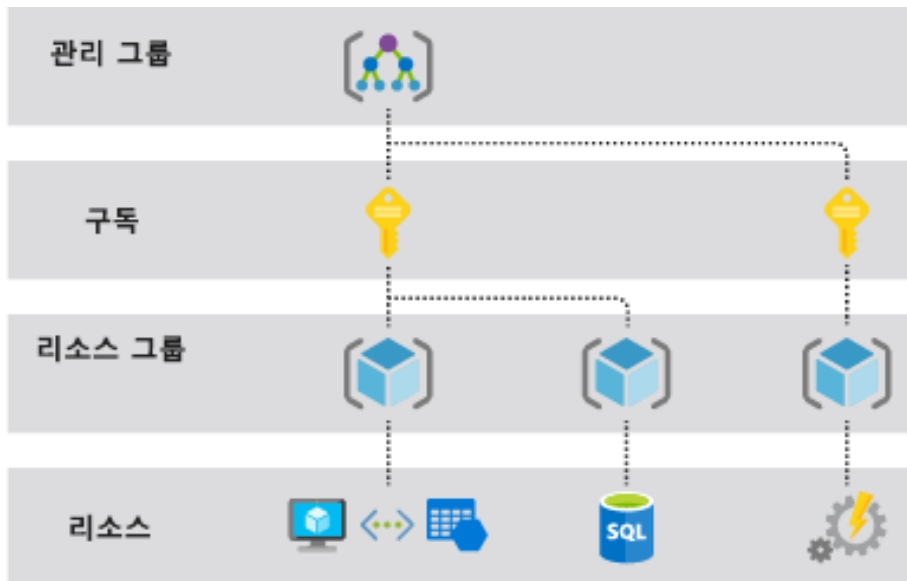
 **Node.js 개발자용 Azure**
시작
API 참조

 **Azure REST API**
API 참조

Resource Manager



Resource Group

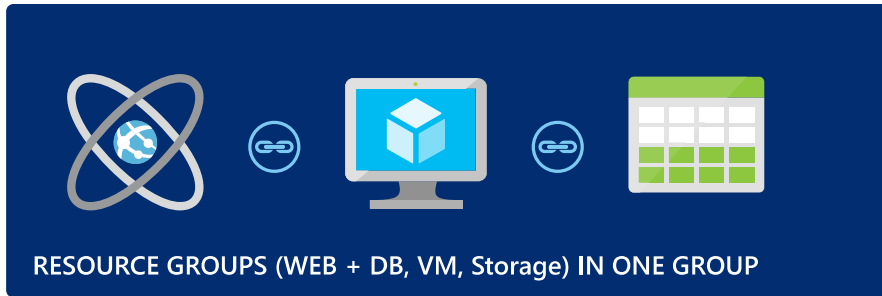


- 리소스 - 관리되는 Azure 항목. 예를 들어 VM, NIC, 저장소 계정
- 리소스 그룹 - 관련된 리소스를 가지고 있는 컨테이너
- 리소스 그룹 - 최대 800개 리소스, 중첩될 수 없음
- 리소스 - 한 리소스 그룹에만 존재할 수 있음
- 리소스 - 리소스 그룹에서 언제든지 추가/제거할 수 있음
- 리소스 그룹 - 다른 지역에 있는 리소스를 포함할 수 있음

Resource Manager

Resource Design:

리소스를 동일한 그룹 혹은 다른 그룹에 배치할 것인가?



OR



고려 사항:

리소스가 공통적인 **라이프사이클**과 **관리**를 가지는가?

Resource Group tags



- 관리가 정의할 수 있는 키:값 쌍. 예를 들어 Sales Project:1
- 리소스 그룹 당 15개 태그
- 태그 이름은 최대 512 문자
- 태그 값은 최대 256 문자
- 리소스 그룹 혹은 리소스에 적용됨. 상속되지 않음

Tagging Tips

Tag by Environment, e.g. dev/test/prod

Tag by Role, e.g. web/cache/DB

Tag by Department, e.g. finance/legal/developer/Infra

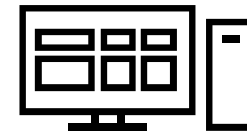


Module 3.

Azure Virtual Machine

Safety, Cost-effective and Powerful

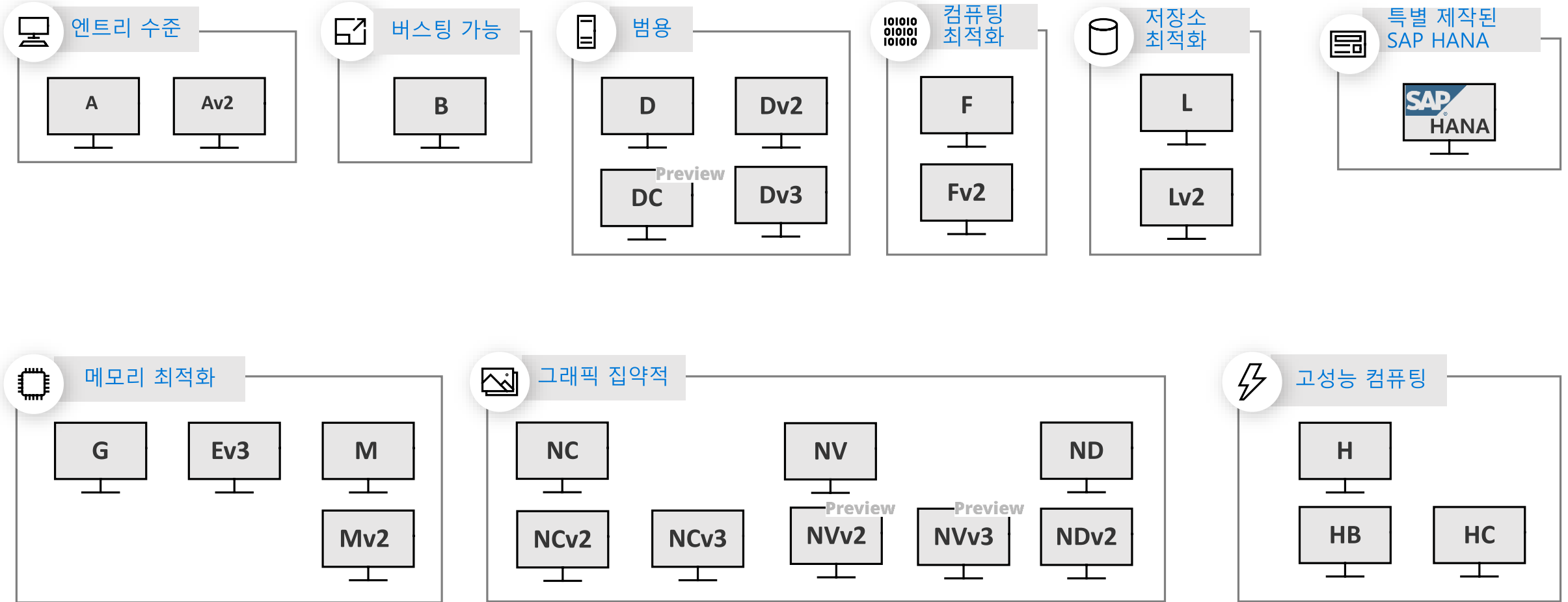
		
<h3>계산</h3>	<h3>저장소</h3>	<h3>네트워킹</h3>
가상 컴퓨터 가용성 집합 VM Scale Set	디스크 (표준, 프리미엄) Blob 저장소 (핫, 쿨) 파일	가상 네트워크, NIC VPN, ExpressRoute LoadBalancer DNS, 트래픽 관리자



관리

- Azure 리소스 관리자(ARM)
- Azure Active Directory
- 포털
- KeyVault
- Azure Backup

Azure Virtual Machine Type



Windows Virtual Machine size: <https://docs.microsoft.com/ko-kr/azure/virtual-machines/windows/sizes>

Azure Virtual Machine Performance

ACU

Azure Compute Unit(ACU)은 Azure SKU 간 컴퓨팅(CPU) 성능을 비교할 수 있는 방법을 제공

크기는 Standard_A1 VM이 100인 상태에서 시작

예제: Dv2-시리즈 CPU가 D 시리즈보다 약 31% 빠름

- *표시가 있는 ACU는 Intel ® Turbo 기술을 사용하여 CPU 주파수를 높이고 성능을 향상 시킴
- Boost 양은 VM 크기, 작업 부하 및 동일한 호스트에서 실행중인 다른 작업 부하에 따라 달라질 수 있음
- **Hyper-threaded.

SKU Family	ACU/vCPU	vCPU:Core
A0	50	1:1
A1 - A4 , A5 - A7 , A1_v2 - A8_v2 , A2m_v2 - A8m_v2	100	1:1
A8 - A11	225*	1:1
D1 - D14	160 - 250	1:1
D1_v2 - D15_v2 , DS1_v2 - DS15_v2	210 - 250*	1:1
DS1 - DS14	160 - 250	1:1
D_v3 , Ds_v3 , E_v3 , Es_v3	160 - 190*	2:1***
F2s_v2 - F72s_v2	195 - 210*	2:1***
F1 - F16 , F1s - F16s	210 - 250*	1:1
G1 - G5 , GS1 - GS5	180 - 240*	1:1
H	290 - 300*	1:1
HB	199 - 216**	1:1
HC	297 - 315*	1:1
L4s - L32s	180 - 240*	1:1
L8s_v2 - L80s_v2	150 - 175**	2:1
M	160 - 180	2:1***

Azure Virtual Machine Performance

CPU Model & Rank

[Azure VM CPU 산정 기준]

Passmark : https://www.cpubenchmark.net/cpu_list.php

VM Type	Hyper-Threading	CPU 1	CPU 2	Intel Turbo Boost Technology 2.0 적용 시	Passmark CPU Mark (higher is better)	Rank (lower is better)
D_v3	Yes	2.4 GHz Intel Xeon® E5-2673 v3(Haswell)	2.3 GHz Intel Xeon® E5-2673 v4(Broadwell)	3.5 GHz	16339/21474	102/40
Ds_v3	Yes	2.4 GHz Intel Xeon® E5-2673 v3(Haswell)	2.3 GHz Intel Xeon® E5-2673 v4(Broadwell)	3.5 GHz	16339/21474	102/40
D_v2	No	2.4 GHz Intel Xeon® E5-2673 v3(Haswell)	2.3 GHz Intel Xeon® E5-2673 v4(Broadwell)	3.1 GHz	16339/21474	102/40
DC*Preview	No	3.7 GHz Intel XEON E-2176G		4.7 GHz	15576	125
F_v2	Yes	2.7 GHz Intel Xeon® Platinum 8168(SkyLake)		3.7 Ghz	29131	2
F	No	2.4 GHz Intel Xeon® E5-2673 v3(Haswell)		3.2 Ghz	16339	102
E_v3	Yes	2.3 GHz Intel XEON® E5-2673 v4(Broadwell)		3.5 GHz	21474	40
G	No	Intel® Xeon® 프로세서 E5 v3				
M	Yes	2.5GHz Intel® Xeon® E7-8890 v3 (Haswell)				
M_v2	Yes	2.5GHz Intel® Xeon® Platinum 8180M (Skylake)			48904	1
L_v2	Yes	AMD EPYC 7551 프로세서(2.55 / 3.0 GHz)			18483	75
L	No	Intel® Xeon® 프로세서 E5 v3				

Azure Virtual Machine

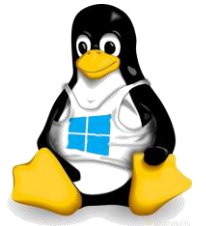
지원되는 게스트 운영 체제

1. Windows Server 2008 R2 SP1 이후 버전

2. 보증되는 Linux 배포판

- Red Hat Linux Enterprise Server 6.7+, 7.2+
- UBUNTU 12.04+ LTS
- CentOS 6.3+, 7.0+
- Debian 7.9+, 8.2+
- Oracle Linux 6.4+, 7.0+
- SUSE Linux Enterprise Server SLES 11 S4+, 12 SP1+ 과 SLES for SAP
- CoreOS 494.4.0+
- OpenSUSE 42.2+

3. FreeBSD





Azure VM 만들기

- 가상네트워크(Virtual Network)
- 가용성 집합(Availability Set)
- 가상컴퓨터
- NSG (Network Security Group)
- 부하분산장치(Load Balancer)
- NIC(Network Interface Card) / IP
- 디스크



Azure Virtual Networks

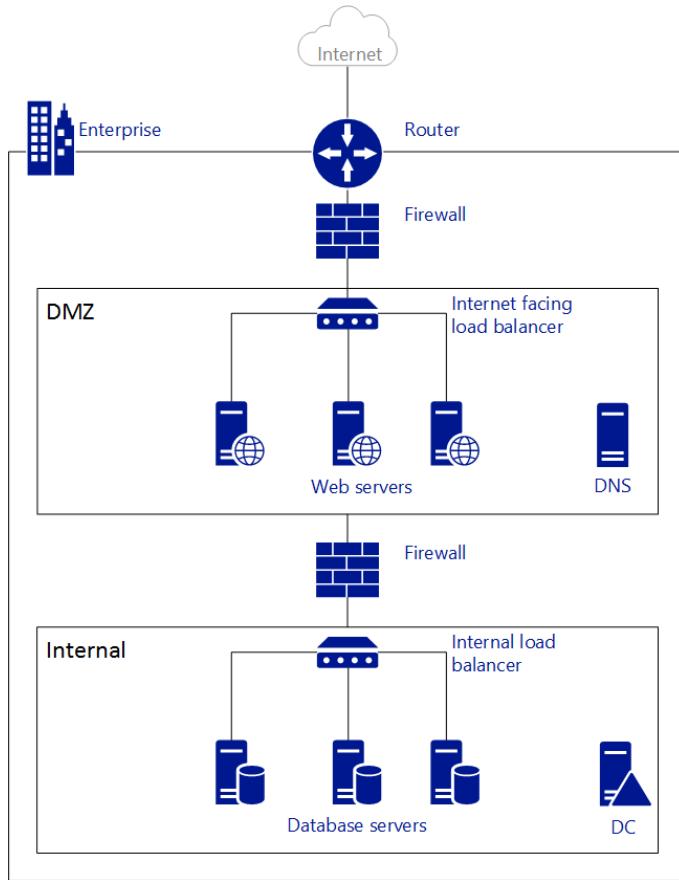


Azure Virtual Networks

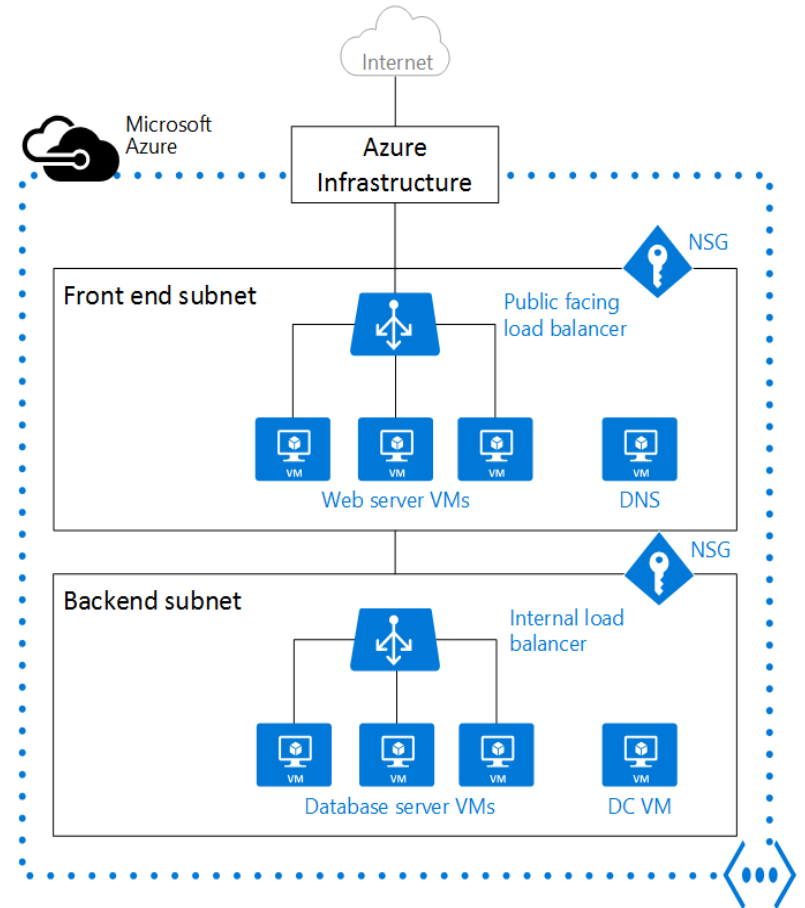
- 가상네트워크 자체는 무료
- 논리적으로 격리되어 있다.
- 가상네트워크간의 기본 통신 불가
- Virtual Network Gateway로 On-Premise 네트워크 연결
- Azure vNet간에 Peering 연결
- 서브넷 간에는 기본 통신 허용

가상 네트워크(Virtual Network)

Azure의 가상네트워크는 On-Premise의 구성과 다르지 않다.



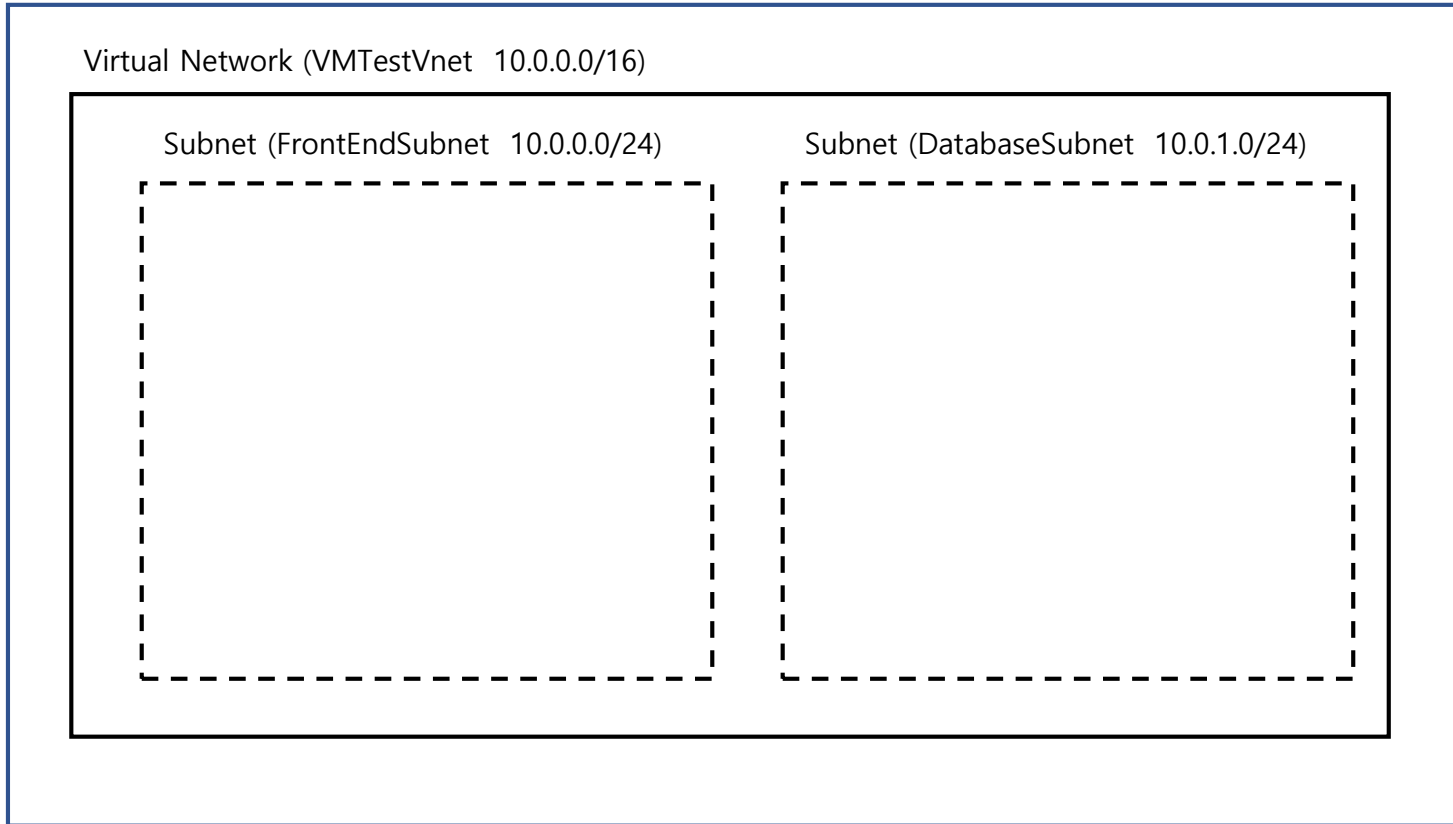
On-Premise 네트워크 구성



Azure 네트워크 구성 Virtual Network

DEMO 1. 가상네트워크 부터 만들자

Resource Group (VMTestGroup)



1. 리소스그룹 생성
2. 가상네트워크 만들기
 - 주소범위지정: 10.0.0.0/24
 - 10.0.0.0-10.0.255.255(65535개)
 - 사용할 수 있는 주소
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
3. 서브넷 만들기
 - 전체 주소중 일부 할당
 - 10.0.0.0/16
 - 10.0.0.1-10.0.0.255(256개)
 - 애플리케이션과 서버구성에 따라서 여러개의 서브넷 구성 가능

주소는 연결해야할 다른 네트워크의 IP주소와 겹치지 않도록 지정

가용성집합(Availability Sets)



Availability Set

- HA구성을 위해 같은 역할을 하는 2개 이상의 VM을 만들 때 필요
- 같은 리소스 그룹에 속한 VM
- AVSet 없이 만든 VM을 나중에 넣을 수 없다.
- VM을 생성할 때 만 AVSet에 넣을 수 있다.
- VM이 한 개 만 있더라도 우선 만들고 VM을 넣자.
- 5 Update Domain / 3 Fault Domain
- Managed Disk 용으로 생성

※ 99.95% 가동 시간 SLA를 달성하기 위해 최소 2 개의 인스턴스가 가용성 집합에 반드시 구현되어야 함

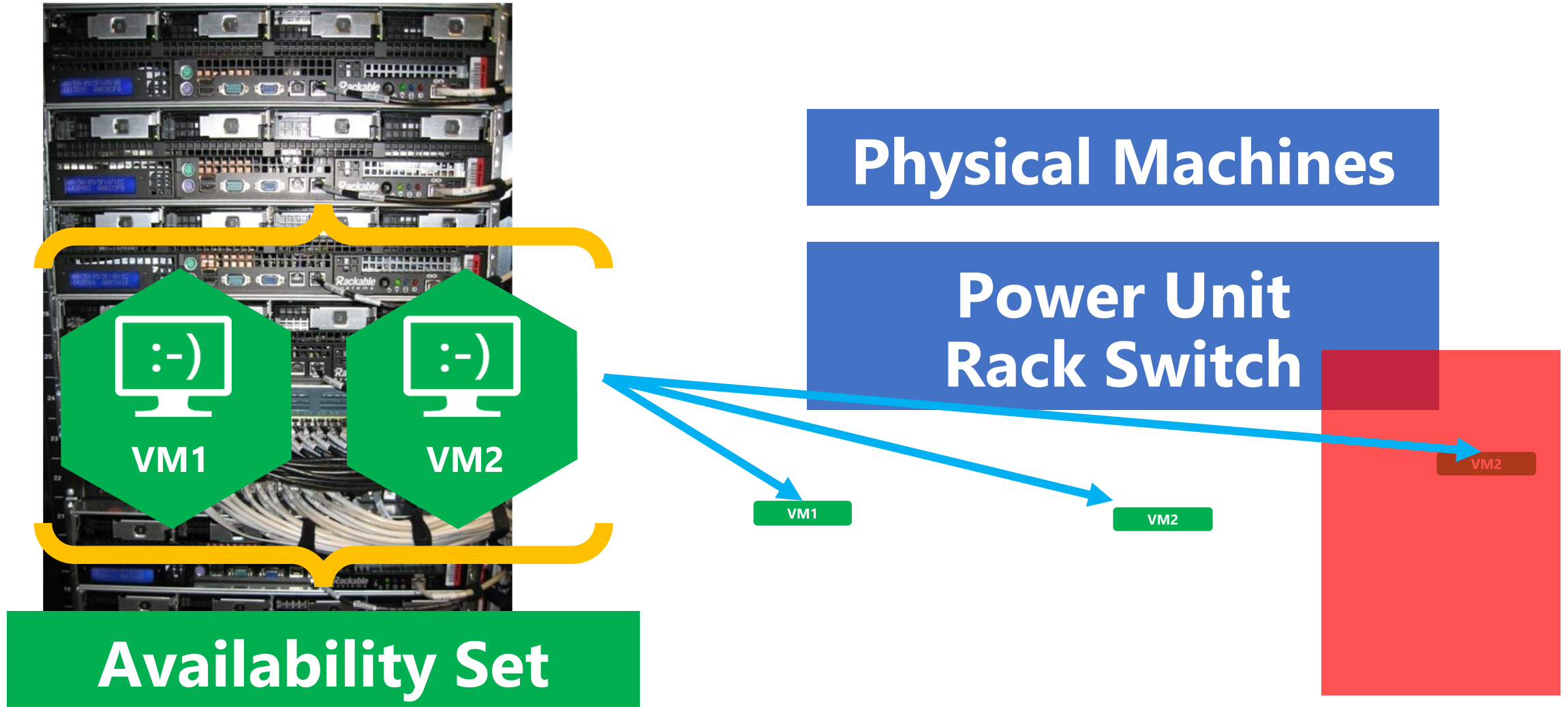
가용성집합(Availability Sets)



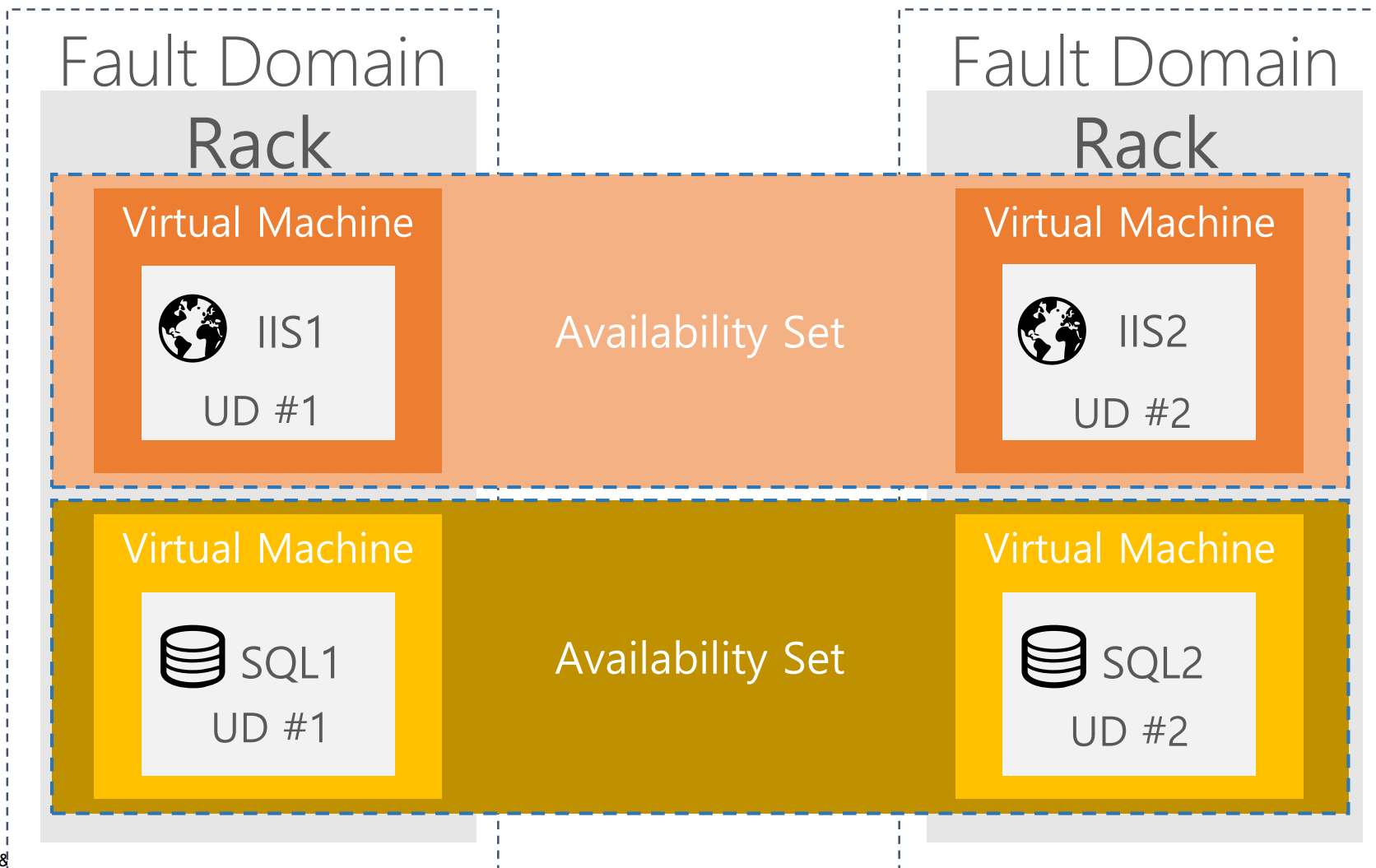
Physical Machines

Power Unit
Rack Switch

가용성집합(Availability Sets)

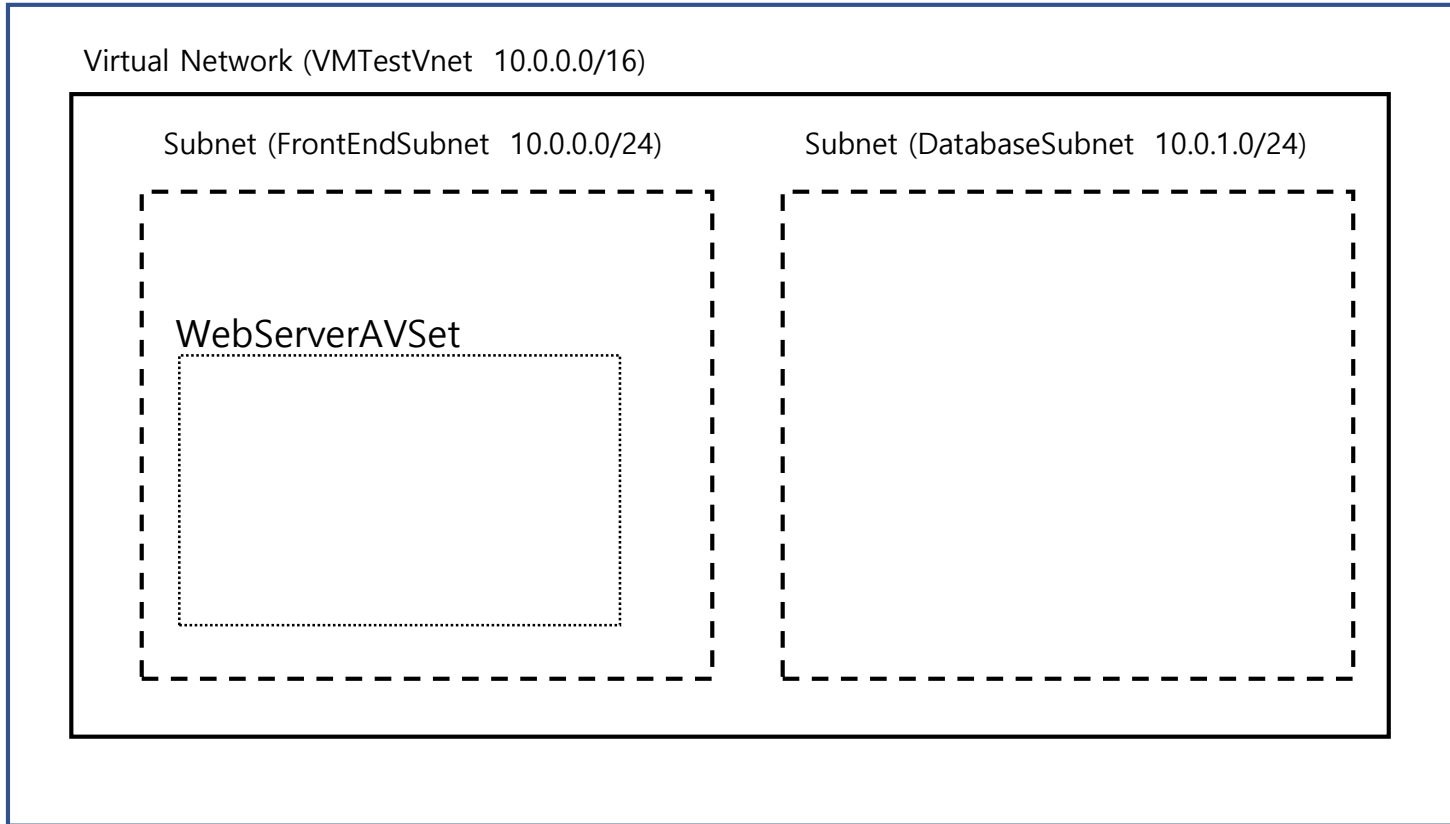


가용성집합(Availability Sets)



DEMO 2. 가용성 집합 생성

Resource Group (VMTestGroup)

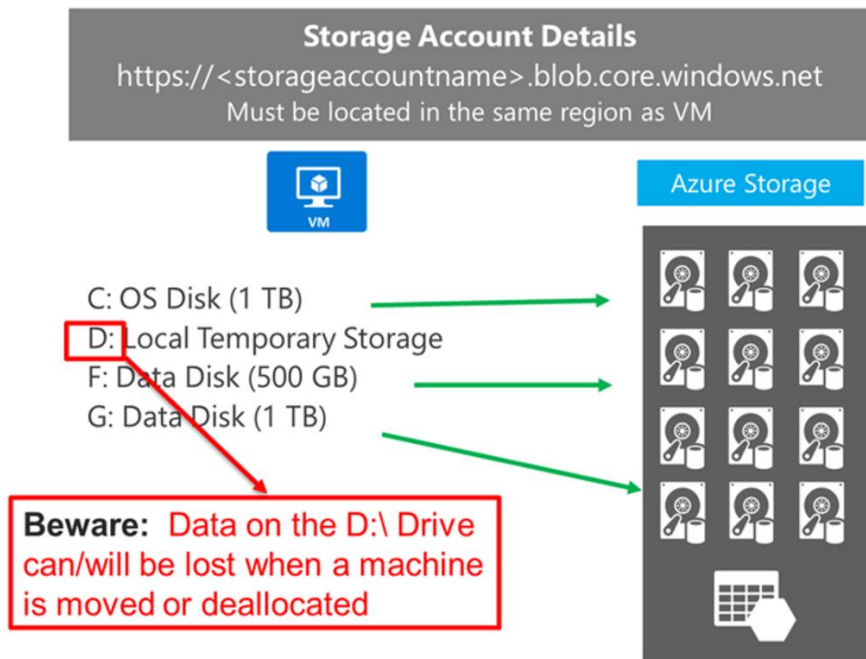


1. 가용성 집합 생성
2. 5 Update Domain
3 Fault Domain
3. Managed Disk 용으로 생성

Managed Disk



Managed Disk



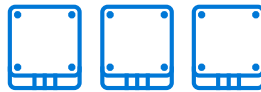
- 가상 컴퓨터 OS와 데이터 디스크는 무작위로 Azure 저장소에 page blob으로 저장됨
- 시작 고정 크기 VHD 형식이 지원됨
- Snapshot, image 생성 가능
- 최대 32 TB 디스크
- 대부분의 Azure 이미지는 30 GB ~ 127 GB 범위의 시스템 볼륨을 가지고 있음
- Non-OS 볼륨은 32 TB 이상의 크기를 가질 수 있고 소프트웨어 RAID를 지원하는 OS를 통해 만들 수 있음

	Windows	Linux
OS 디스크 (blob 저장소)	C:	/dev/sda
임시/리소스 디스크 (로컬 디스크) !⚠ 여기에 아무 것도 저장하지 말 것	D:	/dev/sdb
데이터 디스크 (blob 저장소)	E, F, 등	/dev/sdc, /dev/sdd, 등

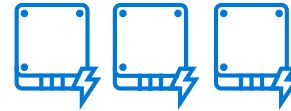
Managed Disk 유형



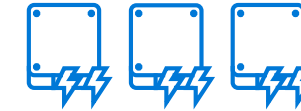
표준 HDD



표준 SSD



프리미엄 SSD



울트라 SSD

미리 보기

낮은 비용의
저장소

일관된 성능

고성능

ms미만의 지연
시간

최대 크기

32 TiB

32 TiB

32 TiB

64 TiB

최대 IOPS

최대 2,000

최대 6,000

20,000

160,000

최대 BW

최대 500 MB/s

최대 750 MB/s

900 MB/s

2,000 MB/s

특징

Virtual Machine



Virtual Machine

Virtual Machine은 2가지 중지된 상태를 지원:

할당 취소 Deallocated

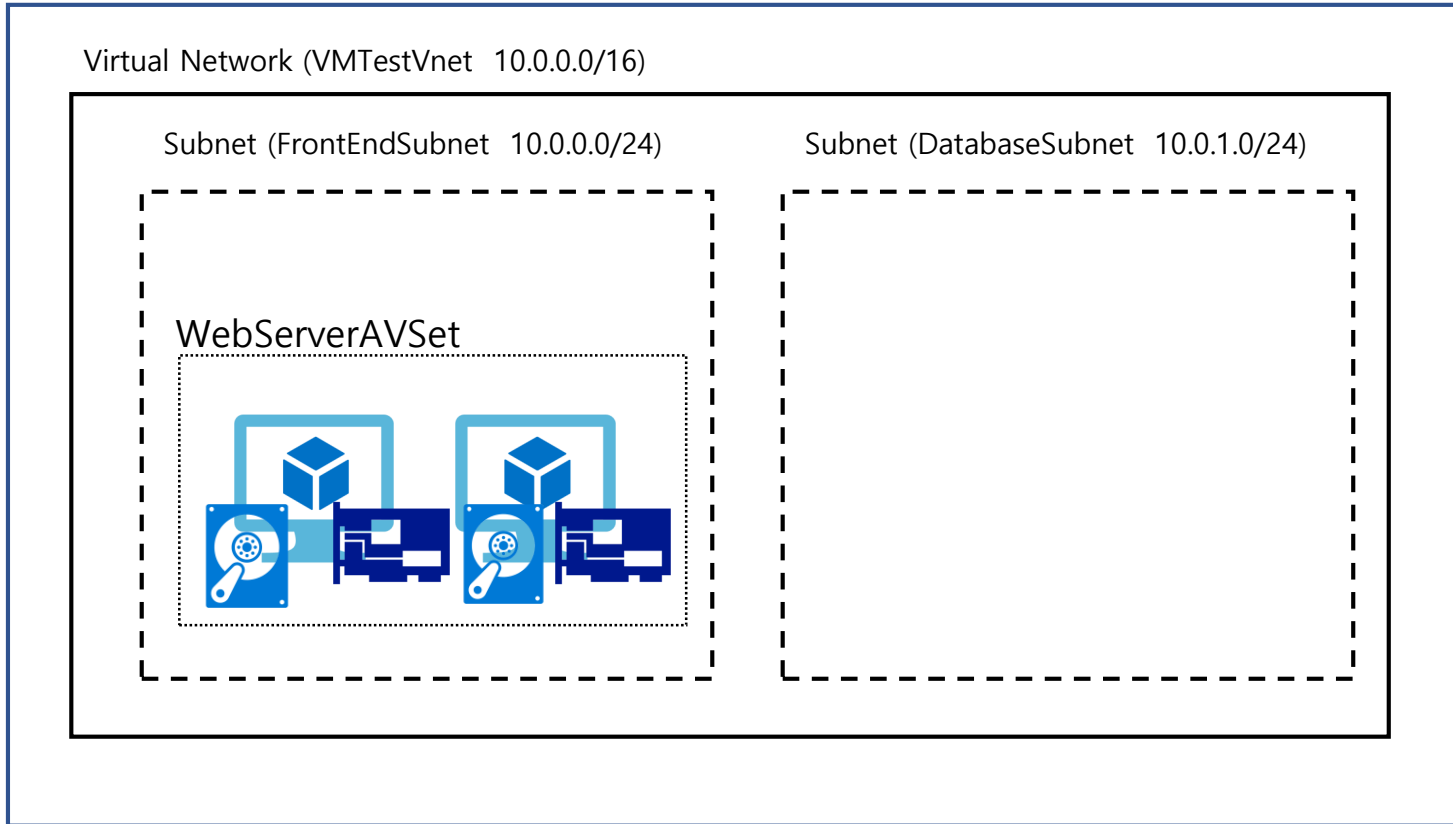
- CPU에 대한 과금 없음 (저장소에 대해서는 과금)
- 정적 IP (공용 혹은 사설)를 사용하지 않은 경우 IP 주소가 유지되지 않음
- 포털 혹은 명령줄 도구를 통해 중지

중지 Stopped

- OS는 꺼지지만 계산에 대한 과금은 계속됨
- OS 내에서 혹은 명령줄 도구 (옵션)를 통해 중지

DEMO 3. VM 만들기 (2개)

Resource Group (VMTestGroup)



1. VM 생성
 - OS
 - SSD / HDD 선택
 - Admin 계정
 - 크기
2. 미리 생성해둔 리소스 붙임
 - VNet / Subnet
 - AVSet
 - **Managed Disk 선택**
 - Public IP / NSG 만들지 **않음**
 - Diagnostic 용 Storage 만들기
3. NIC는 자동으로 생성
 - 지정된 Subnet에 생성
 - VM이름에 랜덤한 번호 붙음

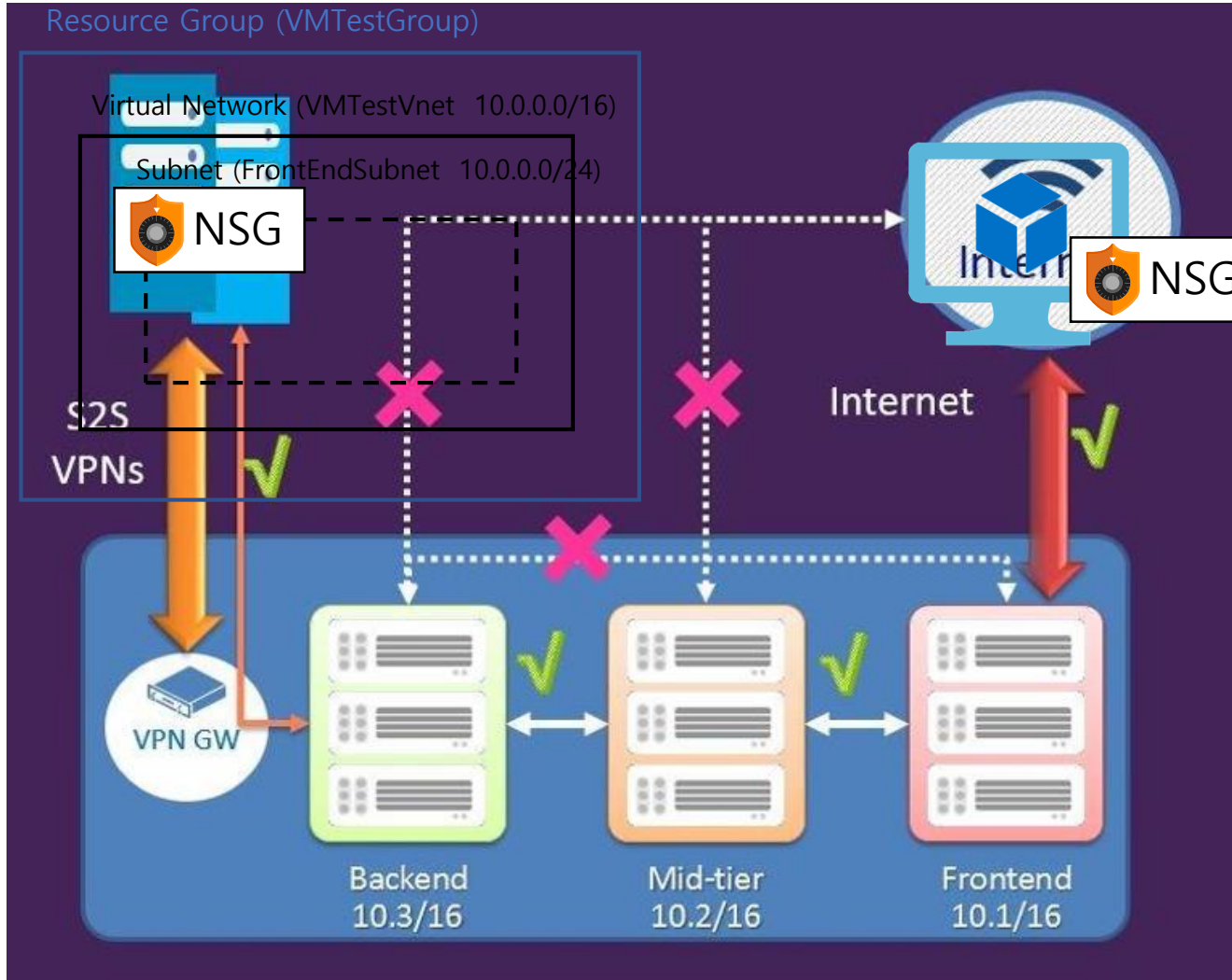
Network Interface



Network Interface

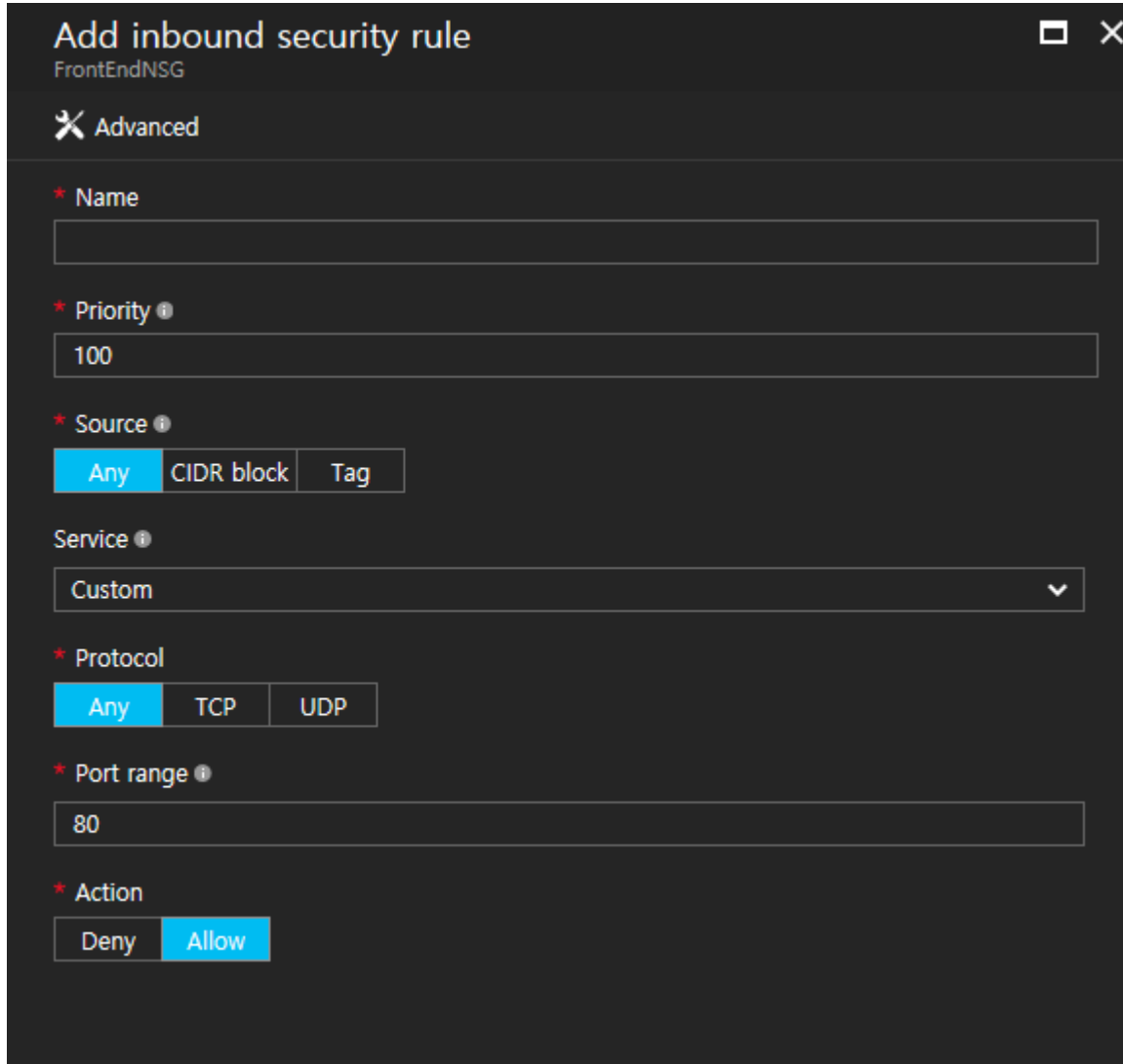
- VM 만들 때 같이 만들어진다.
- 랜덤숫자가 붙는 이름이 싫으면 PowerShell
- 서브넷에 속한다.
- 가상컴퓨터에 붙는다.
- 기본적으로 서브넷의 Private IP를 가진다.
- Private IP를 고정할 수도 있다.
- NSG(Network Security Group)을 가질 수 있다.

NSG (Network Security Group)



- 방화벽 역할
- 가상네트워크의 서브넷이나 VM의 개별 인스턴스에 붙일 수 있다.
- 개별 VM 보다는 서브넷에 붙이는 것이 제어하기 편하다.
- NSG를 잘 활용하면 DMZ를 만들 수 있다.
- 외부 접속은 Frontend 서브넷만 허용
- 나머지 서브넷은 인터넷 연결 차단
- 서브넷 사이는 연결 허용
- Backend 서비스의 On-Premise 연결은 VPN 사용

Azure VM 만들기 NSG 설정



Add inbound security rule
FrontEndNSG

✕ Advanced

* Name

* Priority ⓘ

* Source ⓘ

Service ⓘ

* Protocol

* Port range ⓘ

* Action

- Inbound / Outbound 규칙
- 우선순위
- 소스IP/Port,
Destination IP/Port,
Protocol
- Allow / Deny

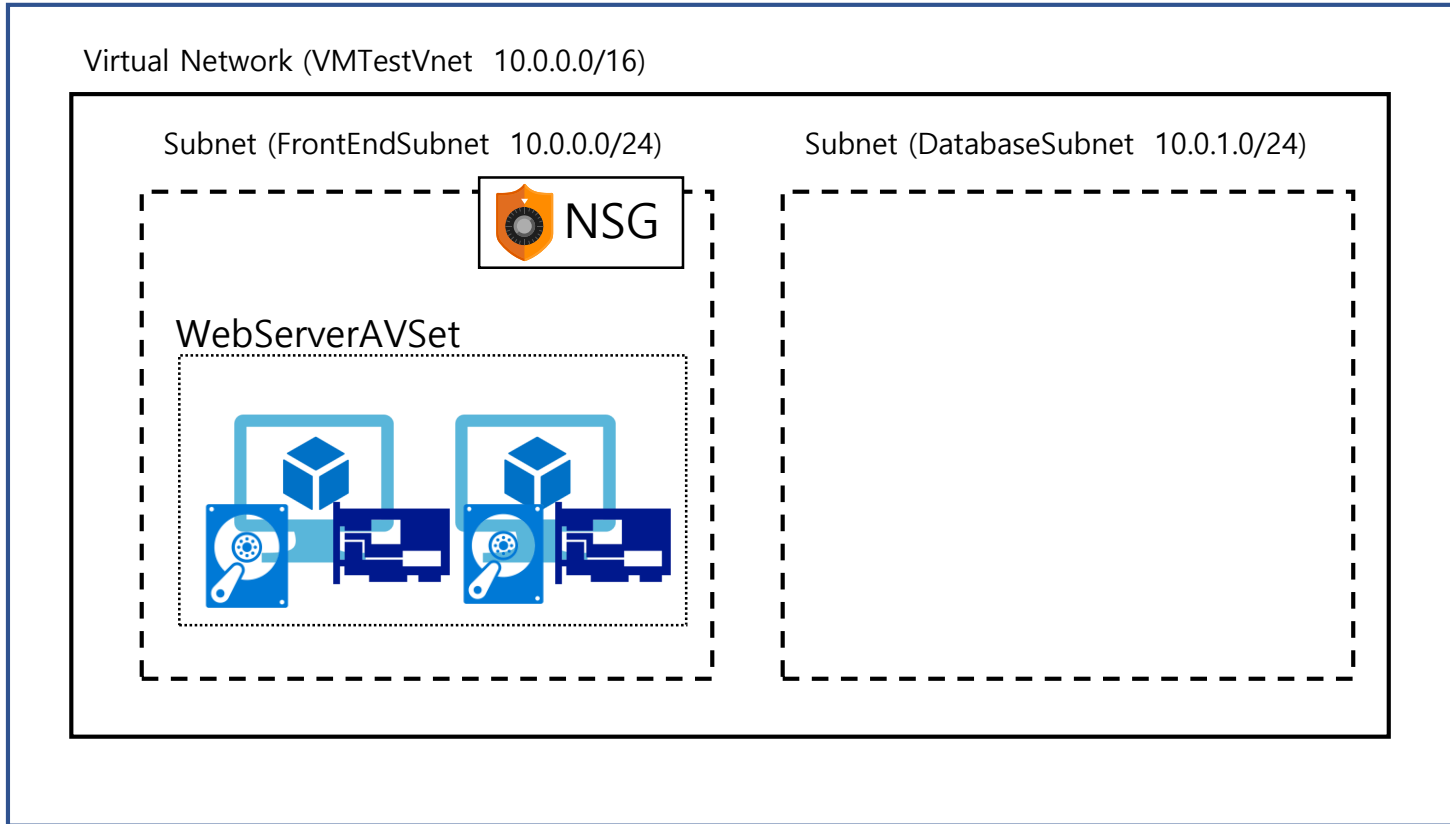
NSG 기본 규칙 (Default Rules)

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION	
65000	AllowVnetInBound	VirtualNetwork	VirtualNetwork	Custom (Any/Any)	Allow	...
65001	AllowAzureLoadBalancerInBound	AzureLoadBalancer	Any	Custom (Any/Any)	Allow	...
65500	DenyAllInBound	Any	Any	Custom (Any/Any)	Deny	...

- 기본규칙이 설정 되어 있다.
- Vnet 안에서는 모두 허용 (AllowVnetInBound)
- 부하분산장치(Load Balancer)에서 오는 건 모두 허용 (AllowAzureLoadBalancerInBound)
- Inbound 모두 거부 (DenyAllInBound)

DEMO 4. FrontEndSubnet에 NSG를 만들자.

Resource Group (VMTestGroup)



1. NSG 생성
2. Default Rule
3. Inbound Rule 생성
 - 80 / HTTP / Allow / Any



Load Balancer

- 4 계층(TCP, UDP) 트래픽 부하분산
- VNet의 VM 사이
- 2가지 종류 인터넷연결(Internet-facing) / 내부(Internal)
- 인터넷연결은 Public IP를 가질 수 있다.
- Probe로 서비스가 살아 있는지 체크
- NAT 규칙 설정

LoadBalancer

Frontend IP Pool / Backend Pools

1) Public IP를 Frontend IP Pool에 등록



2) 가용성집합(Availability Set)에 속한 VM1, VM2 가상컴퓨터를 Backend Pool로 등록



Frontend IP Pool

- 인터넷 연결 타입이라면 Public IP를 여러개 붙일 수 있다.
- 3튜플: IP / Protocol(UDP,TCP)/ Port

Backend Pools

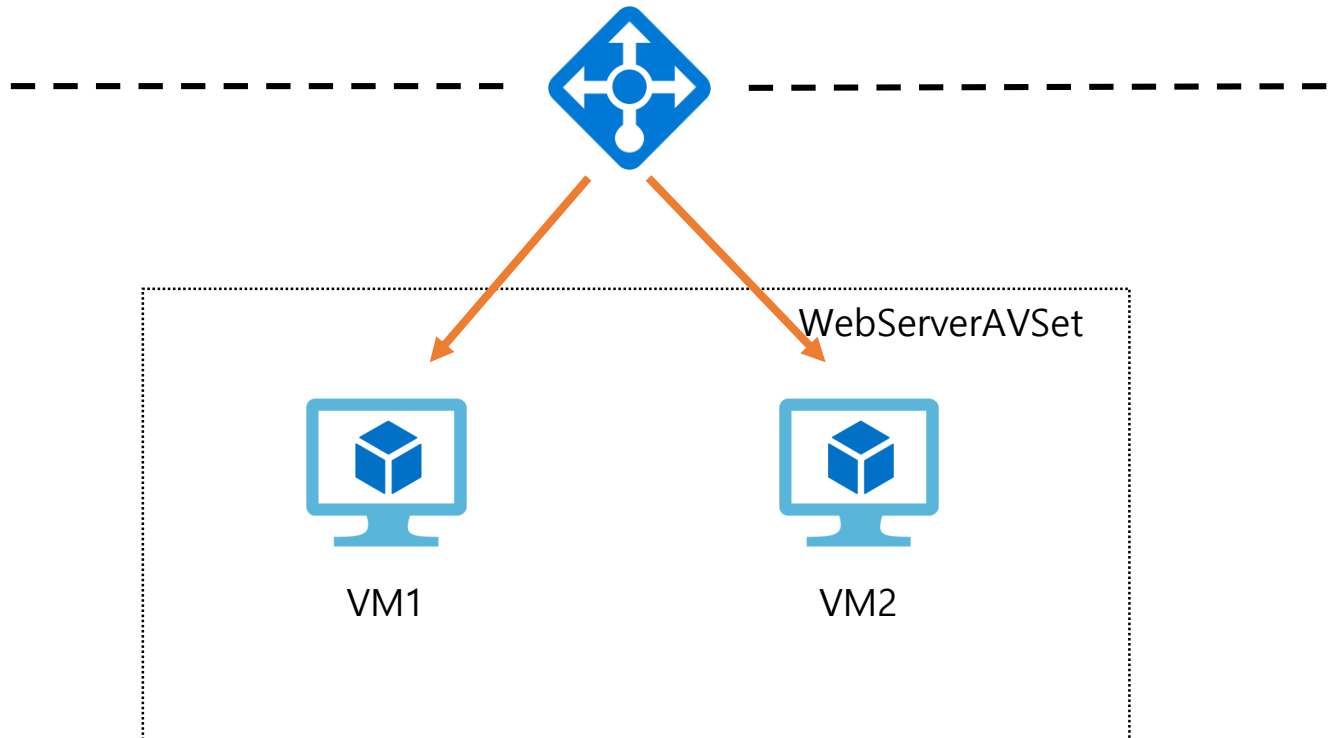
- 가용성집합에 속한 VM들을 하나의 Pool로 묶는다.

LoadBalancer

상태 프로브(Health Probe)

3) Health Probe를 등록

- HTTP 프로토콜 80 포트의 루트패스("/")를 Probe로 등록



기본값

- 주기(Interval): 5초
- 임계값(Unhealthy threshold): 2 연속
- 5초간격을 체크하는데 2번연속 오류일 때 Unhealthy로 판단
- 반대의 경우 다시 연결

HTTP Probe

- HTTP의 경우 Probe용 페이지를 하나 만들어서 간단한 DB Request까지 하면 웹 애플리케이션과 DB가 모두 정상일 때 부하를 받도록 할 수 있다.
- HTTPS는 지원하지 않음
- 200이외의 응답일 때 실패

TCP Probe

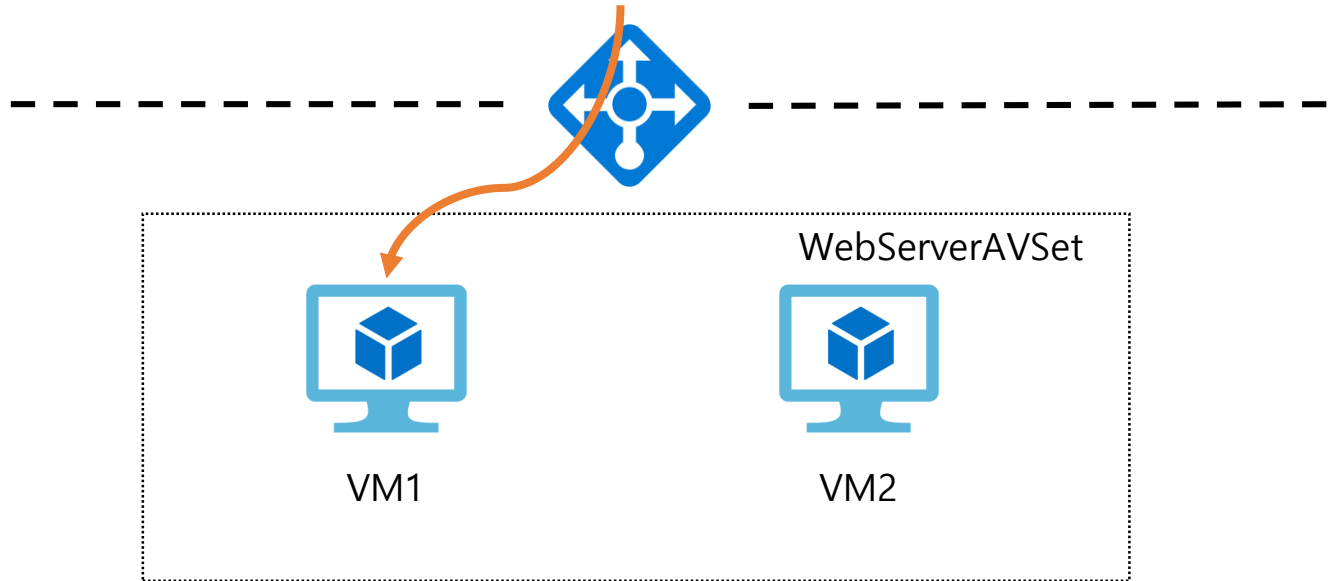
- Time out 발생하면 실패

LoadBalancer

부하분산규칙(Load Balancing Rules)

4) 부하분산규칙 등록

- Frontend IP로 들어온 80포트 TCP 요청을 백엔드 풀의 80로 전달하는데 프로브를 사용하여 상태를 체크하라



- Session Persistence: Session사용을 위해 처음 연결된 VM에 계속 연결
- Idle Timeout 최대 30분으로 설정

The screenshot shows the 'Add load balancing rule' configuration window for 'VMTestLB'. The configuration is as follows:

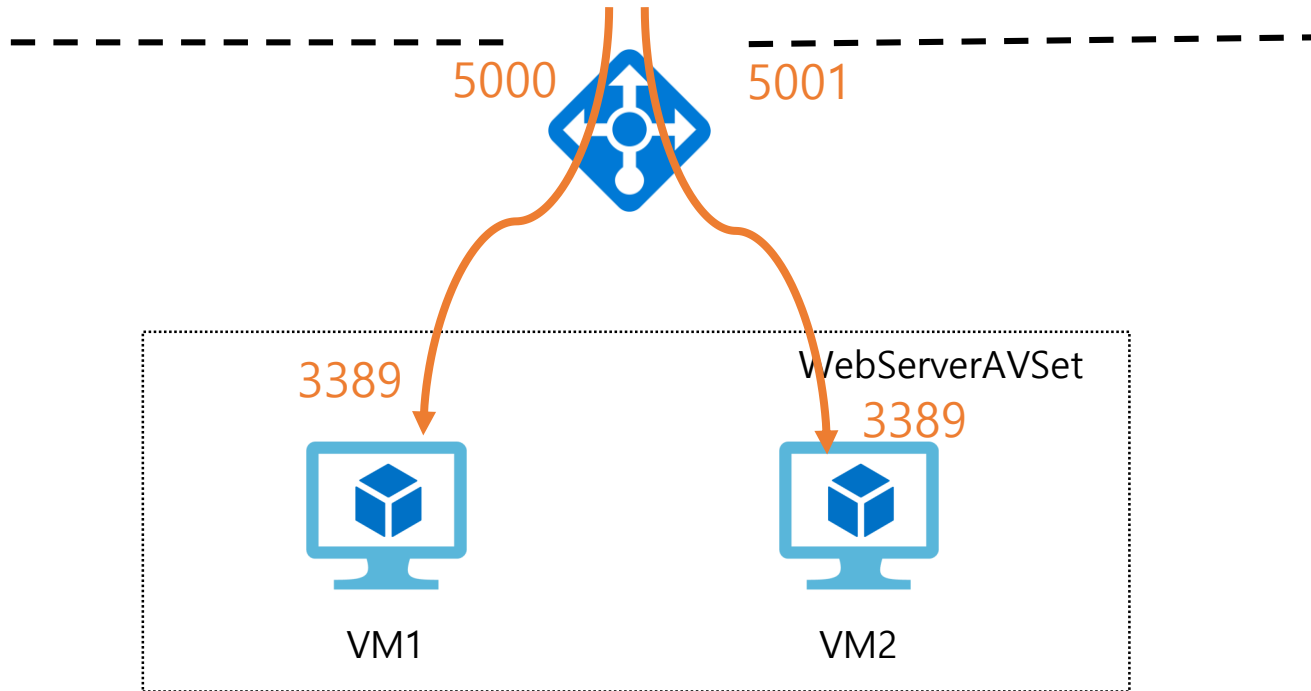
- Name:** HTTPRule
- Frontend IP address:** LoadBalancerFrontEnd
- Protocol:** TCP (selected), UDP
- Port:** 80
- Backend port:** 80
- Backend pool:** WebServerBackendPool (2 virtual machines)
- Health probe:** HttpProbe (HTTP:80)
- Session persistence:** None
- Idle timeout (minutes):** 30
- Floating IP (direct server return):** Disabled (selected), Enabled

LoadBalancer

NAT 규칙(NAT Rules)

5) NAT 규칙 적용

- RDP나 SSH 처럼 백엔드 풀에 있는 개별 VM에 접속하기 위한 NAT 설정
- Frontend IP로 5000번으로 TCP 접속은 VM1의 3389
- Frontend IP로 5001번으로 TCP 접속은 VM2의 3389



The screenshot shows the 'Add inbound NAT rule' configuration page in the Azure portal. The page title is 'Add inbound NAT rule' and the resource is 'VMTestLB'. The instructions state: 'Create an inbound NAT rule to route incoming traffic to a virtual machine in your virtual network.' The configuration fields are as follows:

- Name:** RDPRule
- Frontend IP address:** 52.231.31.112 (LoadBalancerFrontEnd)
- Service:** RDP
- Protocol:** TCP (selected), UDP
- Port:** 5000
- Target:** VM0
- Port mapping:** Custom (selected), Default
- Floating IP (direct server return):** Disabled (selected), Enabled
- Target port:** 3389

LoadBalancer

Standard LB / Basic LB

	Standard LB SKU	Basic LB SKU
백 엔드 풀 크기	최대 1000개 인스턴스를 지원합니다.	최대 100개 인스턴스를 지원합니다.
백 엔드 풀 엔드포인트	단일 가상 네트워크의 가상 머신(가상 머신, 가용성 집합, 가상 머신 확장 집합 혼합 포함).	단일 가용성 집합 또는 가상 머신 확장 집합의 가상 머신.
상태 프로브	TCP, HTTP, HTTPS	TCP, HTTP
상태 프로브 다운 동작	TCP 연결은 인스턴스 프로브 및 모든 프로브가 다운되어 있을 때 그대로 유지됩니다.	TCP 연결은 인스턴스 프로브가 다운되어 있을 때 그대로 유지됩니다. 모든 프로브가 다운되면 모든 TCP 연결이 종료됩니다.
가용성 영역	표준 SKU에서 인바운드 및 아웃바운드, 아웃바운드 흐름 매핑 생존 영역 장애, 영역 간 부하 분산을 위한 영역 중복 및 영역 프런트 엔드.	사용할 수 없음.
진단	Azure Monitor, 바이트 및 패킷 카운터, 상태 프로브 상태, 연결 시도(TCP SYN), 아웃바운드 연결 상태(SNAT 성공 및 실패 흐름), 활성 데이터 평면 측정을 포함하는 다차원 메트릭	공용 Load Balancer 전용, SNAT 소모 경고, 백 엔드 풀 상태 수에 대한 Azure Log Analytics.
HA 포트	내부 부하 분산 장치	사용할 수 없음.
기본적으로 보안 적용	공용 IP, 공용 Load Balancer 엔드포인트, 내부 Load Balancer 엔드포인트는 네트워크 보안 그룹에 의해 허용 목록에 추가되지 않는 한 인바운드 흐름에 대해 닫힙니다.	기본적으로 열려 있는 선택적 네트워크 보안 그룹입니다.
유휴 상태의 TCP 재설정	규칙에서 유휴 시간 제한에 도달하면 TCP 재설정(TCP RST) 사용	사용할 수 없음
여러 프런트 엔드	인바운드 및 아웃바운드	인바운드 전용
관리 작업	대부분 작업을 30초 이내에 수행	일반적으로 60-90+초.
SLA	2개의 정상 가상 머신이 있는 데이터 경로에 대해 99.99%.	사용할 수 없습니다.
가격	규칙 수, 리소스와 관련해서 인바운드 및 아웃바운드로 처리된 데이터에 따라 요금 부과	무료



Public IP

※ 할당 방법을 고정으로 설정한 경우에도 공용 IP 주소 리소스에 할당된 실제 IP 주소를 지정할 수 없습니다. Azure는 리소스가 생성된 Azure 위치에서 사용 가능한 IP 주소 풀의 IP 주소를 할당됩니다.

Basic

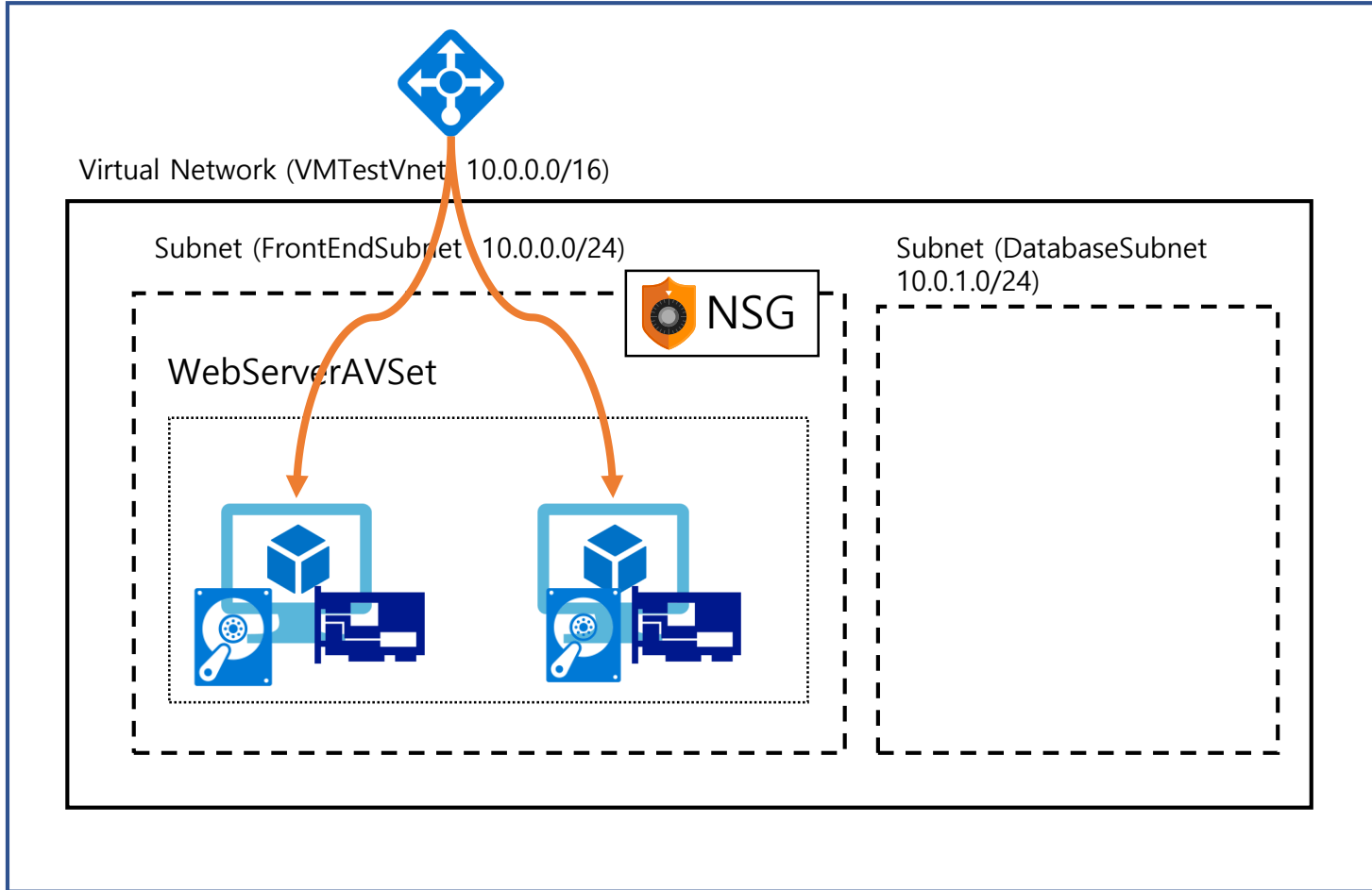
- 동적/고정 IP를 선택할 수 있다.
- Network Interface, LB, VPN Gateway, Application Gateway 등 IP주소를 할당할 수 있는 모든 Azure 리소스에 붙일 수 있다.
- 동적 Public IP는 VM, LB가 시작될 때 IP가 부여되고 중지 또는 삭제하면 IP가 해제된다. 즉, 변경될 수 있다.
- 고정으로 설정하면 삭제하기 전에는 변경되지 않는다.
- 기본적으로 열려 있습니다. NSG를 사용하는 것이 좋지만 인바운드 또는 아웃바운드 트래픽을 제한하는 것은 선택 사항이다.

Standard












- 항상 고정 IP를 할당 받는다.
- Network Interface, Standard LB, VPN Gateway, Application Gateway에 붙일 수 있다.
- TCP Idle Timeout을 기본 4분에서 최대 30분까지 늘릴 수 있다.
- 기본적으로 보호되고 인바운드 트래픽에 닫혀 있습니다. NSG를 사용하여 허용된 인바운드 트래픽을 명시적으로 허용해야 한다.

DEMO. 부하분산장치를 붙이자.

Resource Group (VMTestGroup)



1. VM에 IIS 설정(웹서버)
2. 부하분산장치 생성
 - Frontend IP Pool 설정
 - Backend Pool 설정
 - Probe 설정
 - Load Balancing Rule 설정

 WebServerAVSet	Availability set	대한민국 중부	...
 VM0	Disk	대한민국 중부	...
 VM2	Disk	대한민국 중부	...
 VMTestLB	Load balancer	대한민국 중부	...
 vm0523	Network interface	대한민국 중부	...
 vm2641	Network interface	대한민국 중부	...
 FrontEndNSG	Network security group	대한민국 중부	...
 VMTestPIP	Public IP address	대한민국 중부	...
 VM0	Virtual machine	대한민국 중부	...
 VM2	Virtual machine	대한민국 중부	...
 VMTestVNet	Virtual network	대한민국 중부	...

순서를 기억해주세요.

1. 가상네트워크 / 서브넷
2. 가용성집합
3. 서브넷에 네트워크보안그룹
4. 가상컴퓨터1,2
5. 부하분산장치
 1. Frontend Pool
 2. Backend Pool
 3. Probe
 4. Load Balancing Rule
 5. NAT



Module 4.

Azure Storage Service

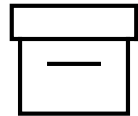
Azure Storage Service



디스크 저장소

프리미엄 및 표준

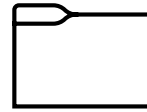
가상 머신을 위한
안정적이고 영구적인
고성능 저장소



개체 저장소

Azure Blobs

백업 및 재해 복구를 위한
안전한 중앙 집중식 저장소



파일 저장소

Azure Files

파일 공유가 필요한 기존
응용 프로그램을
클라우드로 이전



데이터 전송

Azure 가져오기/내보내기
Azure DataBox

데이터를 Azure로 이동
또는 마이그레이션



하이브리드 저장소

Azure StorSimple
Azure File Sync

온-프레미스와 클라우드
저장소 간에 안전하고
지능적인 데이터 계층화

Storage Account

Blob

높은 확장성, REST 기반 클라우드 개체 저장소

- 브라우저에 이미지 또는 문서 직접 제공
- 분산 액세스용 파일 저장
- 동영상 및 오디오 스트리밍
- 백업/복원, 재해 복구 및 보관용 데이터 저장
- 온-프레미스 또는 Azure 호스팅 서비스에 의한 분석용 데이터 저장

HTTP 또는 HTTPS를 통해 어디에서도 액세스

테이블

대규모 자동-스케일링 NoSQL 저장소

로드에 기반한 동적 스케일링

테이블 데이터의 PB로 확장

빠른 key/value 조회

큐

클라우드 서비스를 위한 대규모의 신뢰할 수 있는 큐

구성 요소 decouple과 크기 조정

신뢰할 수 없는 dequeuer로부터 보호하기 위한 메시지 가시성 타임 아웃과 메시지 업데이트

큐 메시지의 크기는 최대 64KB

디스크

Azure IaaS VM을 위한 영구적인 디스크

page blob에 내장

프리미엄 저장소 디스크 : SSD 기반, 높은 IOPS, 낮은 지연

파일

표준 SMB(서버 메시지 블록) 프로토콜을 사용하여 액세스할 수 있는고가용성 네트워크 파일 공유

SAS(공유 액세스 서명) 토큰을 포함하고 있는 URL을 사용

코드 대응(REST API)

Windows & Linux VM에서 사용

Storage Account type

스토리지 계정 형식	지원되는 서비스	지원되는 성능 계층	지원되는 액세스 계층	복제 옵션	배포 모델	암호화 ¹
범용 V2	Blob, 파일, 큐, 테이블 및 디스크	표준, 프리미엄 ⁴	핫, 쿨, 보관 ²	LRS, ZRS ³ , GRS, RA-GRS, ZGRS(preview), RA-ZGRS(preview)	Resource Manager	암호화됨
범용 V1	Blob, 파일, 큐, 테이블 및 디스크	표준, 프리미엄 ⁴	N/A	LRS, GRS, RA-GRS	Resource Manager, 클래식	암호화됨
블록 blob 저장소	Blob(블록 Blob 및 추가 Blob만)	Premium	N/A	LRS	Resource Manager	암호화됨
FileStorage	파일만	Premium	N/A	LRS	Resource Manager	암호화됨
Blob Storage	Blob(블록 Blob 및 추가 Blob만)	표준	핫, 쿨, 보관	LRS, GRS, RA-GRS	Resource Manager	암호화됨

- 1) 모든 저장소 계정은 미사용 데이터에 대해 SSE(저장소 서비스 암호화)를 사용하여 암호화됩니다.
- 2) 보관 계층은 저장소 계정 수준이 아니라 개별 Blob 수준에서만 사용할 수 있습니다. 블록 Blob 및 추가 Blob만 보관할 수 있습니다.
- 3) ZRS(영역 중복 저장소)는 표준 범용 V2 저장소 계정에만 사용할 수 있습니다.
- 4) 범용 v2 및 범용 v1 계정에 대한 프리미엄 성능은 디스크 및 페이지 blob에만 사용할 수 있습니다.

Storage Durability

로컬 중복 저장소 (LRS)

- 여러 데이터 복사본을 하나의 데이터 센터에서 유지하는 방식
- 디스크, 노드, 랙 오류에 대한 데이터 내구성을 제공

영역 중복 저장소 (ZRS)

- 단일 지역에 있는 3개의 스토리지 클러스터에서 데이터를 동기적으로 복제
- 각 스토리지 클러스터는 다른 클러스터와 물리적으로 분리
- 디스크, 노드, 랙 오류에 대한 데이터 내구성을 제공

지역 중복 저장소 (GRS)

- 여러 데이터 복사본을 한 지역에서 유지하고 두 번째 지역으로 비동기식으로 복제하는 방식
- 주요한 지역적 자연 재해에 대해 데이터를 보호하는 추가적인 내구성을 제공

읽기 액세스가 되는 지역 중복 저장소 (RA-GRS)

- GRS에 사용되는 두 번째 지역에서 읽기 권한을 허용하는 방식
- 주요한 지역적 자연 재해에 대해 데이터를 보호하는 추가적인 내구성을 제공
- 지역 간 업데이트는 비동기식으로 수행됨

Azure Blob

Azure Blob, GPv2



핫

자주 액세스하는 데이터



쿨

액세스 빈도가 낮은 데이터



아카이브

거의 액세스 하지 않는 데이터



월 TB당

\$18.40

\$10.00

\$2.00



10k당

읽기/쓰기 비용

\$0.04/\$0.05

\$0.10 / \$1.0

\$50.0 / \$1.0



검색 시간

즉각

즉각

Hours

사용 사례

클라우드 기본 응용 프로그램
데이터

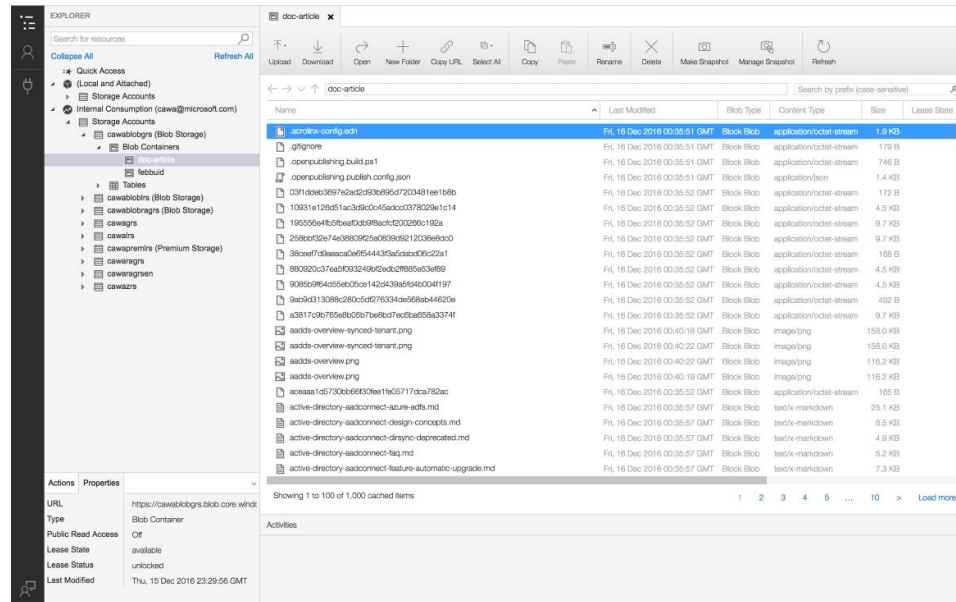
서버 백업

의료 기록 보관

Storage를 위한 Tools



PowerShell, CLI



Azure Storage Explorer

```
Microsoft Azure Storage tools
Microsoft Azure Storage tools
Type azcopy /? for help on AzCopy.

C:\Program Files (x86)\Microsoft SDKs\Azure>azcopy /?
-----
AzCopy 7.1.0 Copyright (c) 2017 Microsoft Corp. All Rights Reserved.
-----

AzCopy </Source:> </Dest:> [/SourceKey:] [/DestKey:] [/SourceSAS:] [/DestSAS:]
[/:] [/:] [/@:] [/:] [/:] [/:] [/:] [/:] [/:] [/:] [/:] [/:] [/:] [/:] [/:] [/:]
[/Pattern:] [/CheckMD5] [/L] [/MT] [/XN] [/XO] [/A] [/IA] [/XA]
[/SyncCopy] [/SetContentType] [/BlobType:] [/Delimiter:] [/Snapshot]
[/PKRS:] [/SplitSize:] [/EntityOperation:] [/Manifest:]
[/PayloadFormat:]

##
## Common Options ##
##

/Source:<source> Specifies the source data from which to copy.
The source can be a directory including:
a file system directory, a blob container,
a blob virtual directory, a storage file share,
a storage file directory, or an Azure table.
The source can also be a single file including:
a file system file, a blob or a storage file.
The source is interpreted according to following rules:
```

AzCopy



Cloud Combine



Gladinet



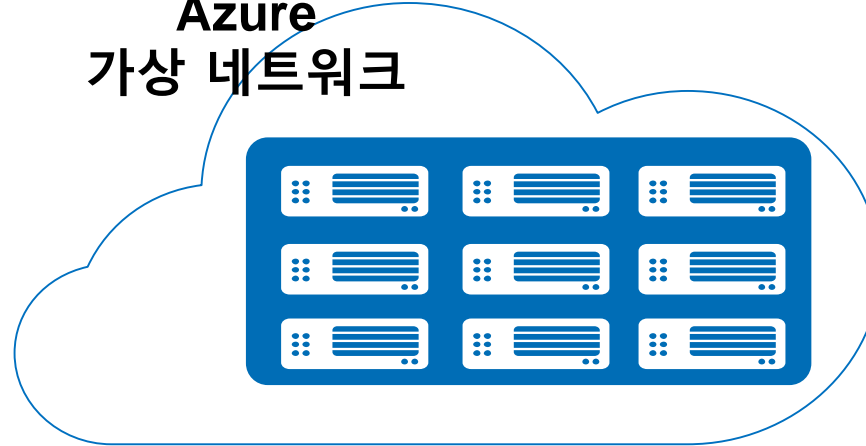
Module 5.

Azure Network

Azure Network Service



Azure 가상 네트워크

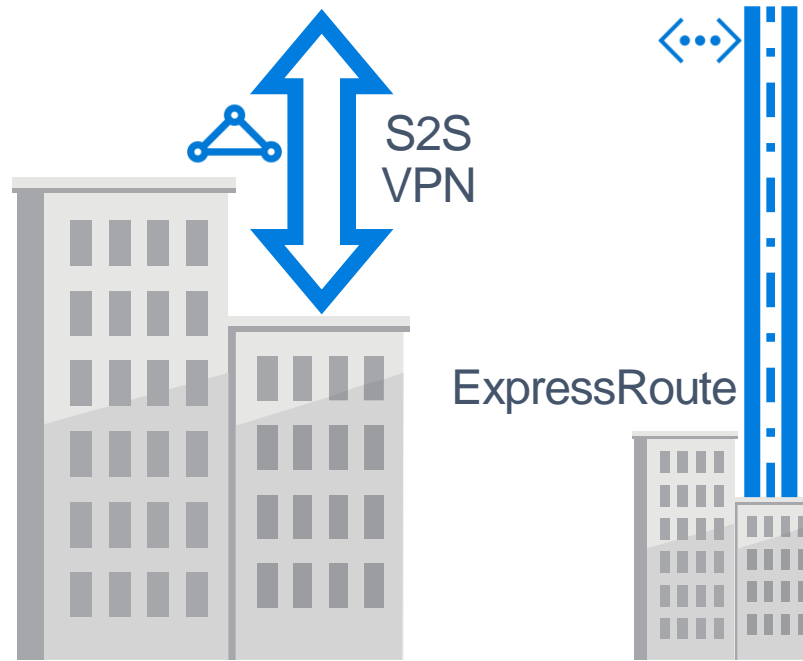


Virtual Network

- “Bring Your Own Network”
- 서브넷과 네트워크 보안 그룹으로 세그먼트
- 사용자 정의 경로로 트래픽 제어

Frontend access

- 동적/예약된 공용 IP 주소
- 직접 VM 액세스, 보안을 위한 ACL
- 로드 밸런싱 & 응용 프로그램 게이트웨이
- DNS 서비스: 호스팅, 트래픽 관리
- DDoS 보호



Backend access

- 개발/테스트를 위한 Point-to-Site - ssl
- 안전한 Site-to-Site 연결을 위한 VPN 게이트웨이 - ipsec
- 사설 엔터프라이즈 수준의 연결을 위한 ExpressRoute - 전용

Azure Network Service



가상 네트워크

사설 네트워크를 제공하고 필요에 따라 온-프레미스의 데이터 센터로 연결



로드 밸런서

응용프로그램에 고가용성 및 네트워크 성능을 제공



응용 프로그램 게이트웨이/WAF

Azure에 확장 가능하고 가용성이 높은 웹 프론트 엔드 구축



DDoS 보호

DDoS 공격으로부터 Azure 리소스 보호



VPN 게이트웨이

안전한 Cross-프레미스 연결을 구축



Azure DNS

Azure에서 DNS 도메인을 호스팅



Content Delivery Network

글로벌한 범위에서 안전하고 신뢰할 수 있는 콘텐츠 전달을 보장



트래픽 관리자

가용성과 고성능을 위한 최신 트래픽 경로



ExpressRoute

Azure 전용 사설 네트워크 연결

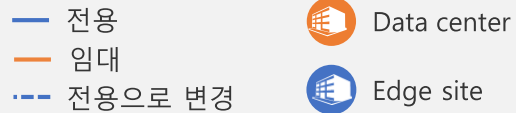
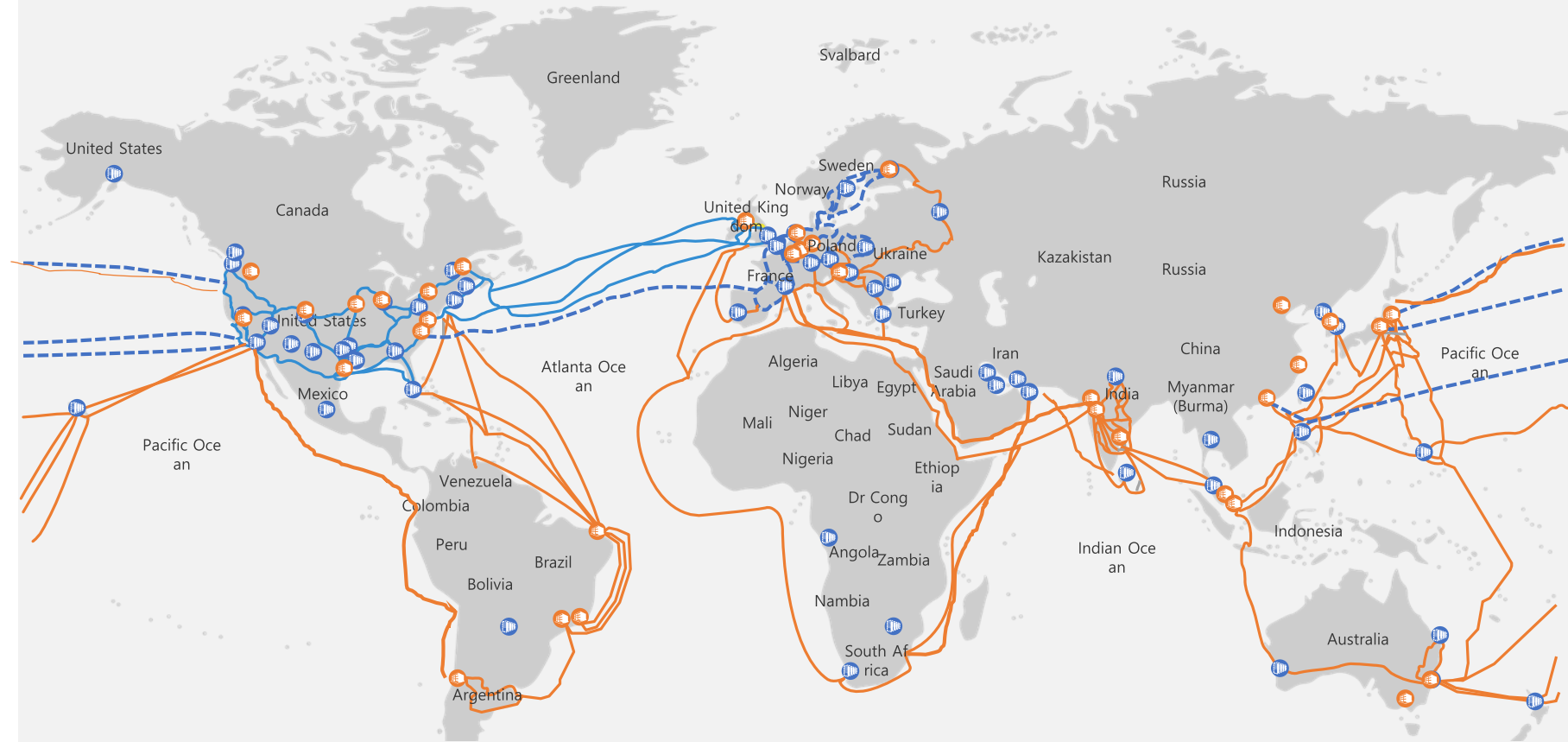


Network Watcher

네트워크 성능 모니터링 및 진단 솔루션

Microsoft 글로벌 네트워크

- 세계에서 가장 큰 사설 네트워크 중 하나
- 8,000+ ISP 세션
- 130+ 경계 사이트
- 44개의 ExpressRoute 위치
- 33,000 마일의 광섬유
- SDN 관리(SWAN, OLS)



Azure Load Balancer

Public Load Balancer

공용 Load Balancer는 들어오는 트래픽의 Public IP 주소 및 포트 번호를 VM의 Private IP 주소 및 포트 번호로 매핑하며 반대의 경우도 마찬가지입니다.

Automatic reconfiguration

인스턴스를 위 또는 아래로 확장 할 때 즉시 재구성됩니다.

Outbound connections (SNAT)

가상 네트워크 내부의 사설 IP 주소에서 인터넷의 공용 IP 주소로의 모든 아웃바운드 플로우 는 Load Balancer의 프론트 엔드 IP 주소로 변환 될 수 있습니다.

Default Distribution Mode

Azure Load Balancer는 여러 VM간에 트래픽을 균등하게 분배합니다.

Internal Load Balancer

내부 Load Balancer는 가상 네트워크 내에 있거나 VPN을 사용하여 Azure 인프라에 액세스하는 자원으로만 트래픽을 보냅니다.

Cross-premises virtual network

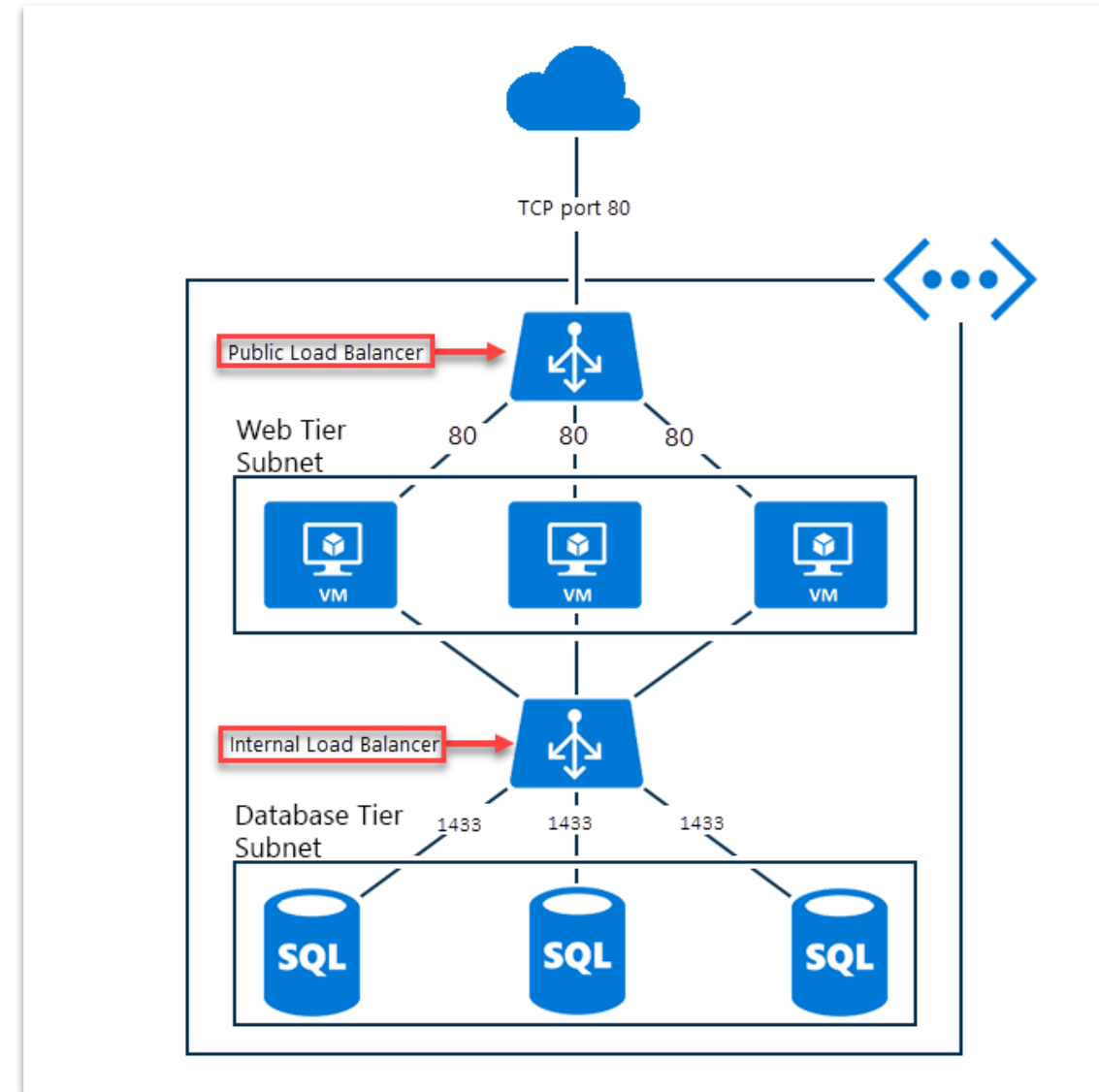
온프레미스 컴퓨터에서 동일한 가상 네트워크 내에 있는 VM에 대한 부하 분산

Multi-tier applications

백엔드 계층이 인터넷에 연결되어 있지 않은 인터넷 연결 다중 계층 응용 프로그램에 대한 부하 분산

Line-of-business applications

추가 HW LB 또는 소프트웨어 없이 Azure에서 호스팅 되는 LOB 응용 프로그램에 대한 부하 분산



Application Gateway

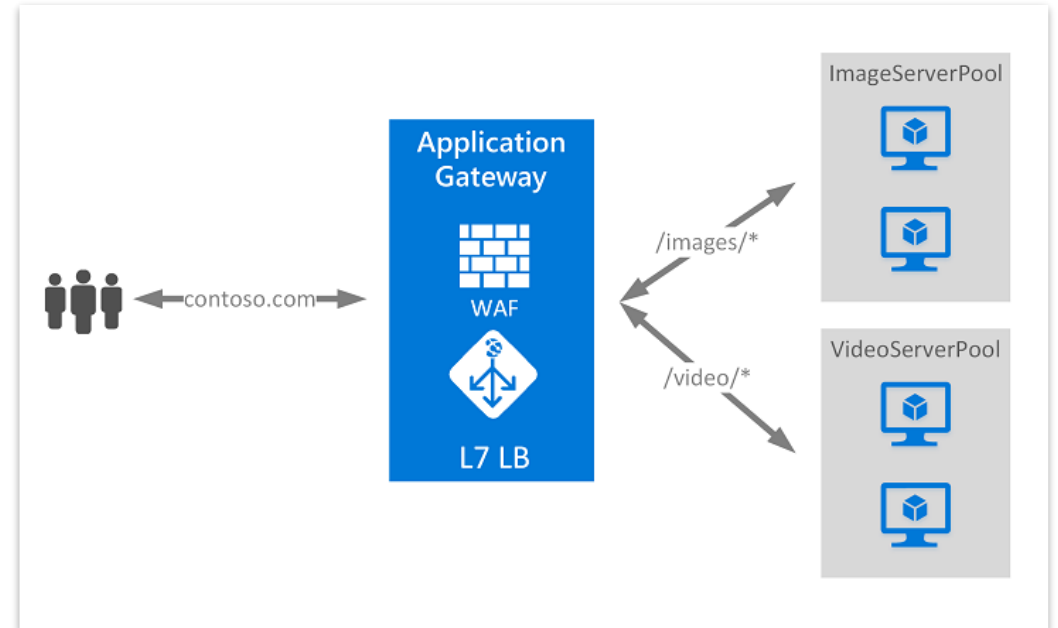
소프트웨어 L7 로드 밸런서

응용 프로그램 수준 정책을 기반으로 하는 HTTP 라우팅:

- HTTP 로드 밸런싱
- 쿠키 기반 세션 선호도
- Secure Sockets Layer (SSL) 오프로드
- URL 기반 콘텐츠 라우팅
- 다중 사이트 라우팅

SSL Termination 캐싱

- 중앙 집중식 인증서 관리



Azure Traffic Manager

DNS 기반 로드 밸런싱

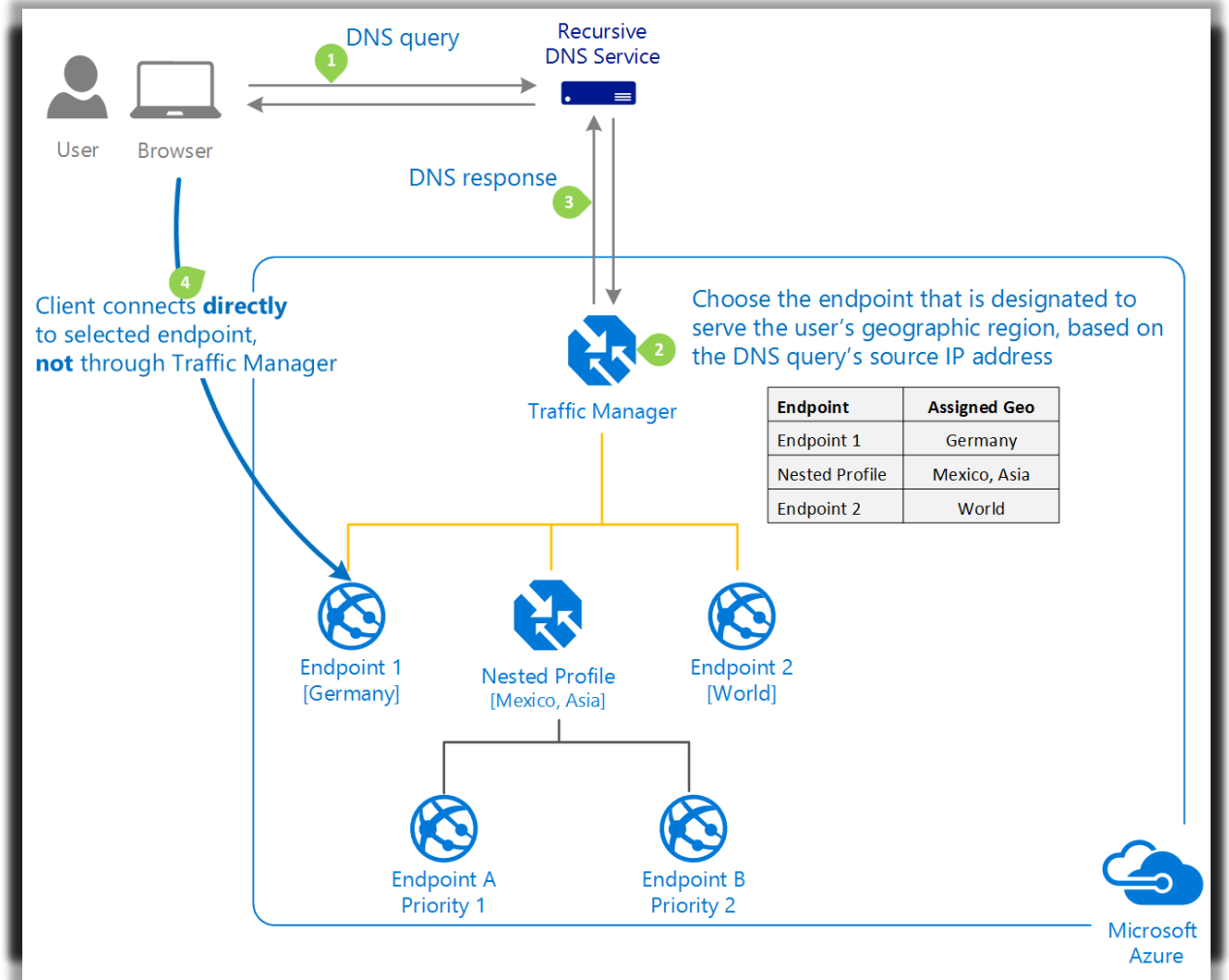
CNAME DNS 레코드와 작동

트래픽 관리자에서 세가지의 트래픽 라우팅 방법:

- 우선 순위: 기본 엔드포인트를 사용할 수 없는 경우 백업 엔드포인트를 제공
- 가중치: 균등 또는 가중치에 따라 엔드포인트 집합에 분산
- 성능: 서로 다른 지리적 위치에 엔드포인트가 있을 때 사용자는 "가장 가까운" 엔드포인트를 사용
- 지리적: 지역 또는 지역 집합이 엔드포인트에 할당된 경우 특정 지역의 요청은 해당 엔드포인트에만 라우트됨

다음 항목에 대해 게시 가능:

- VM
- Azure 웹 응용 프로그램
- 외부 엔드포인트

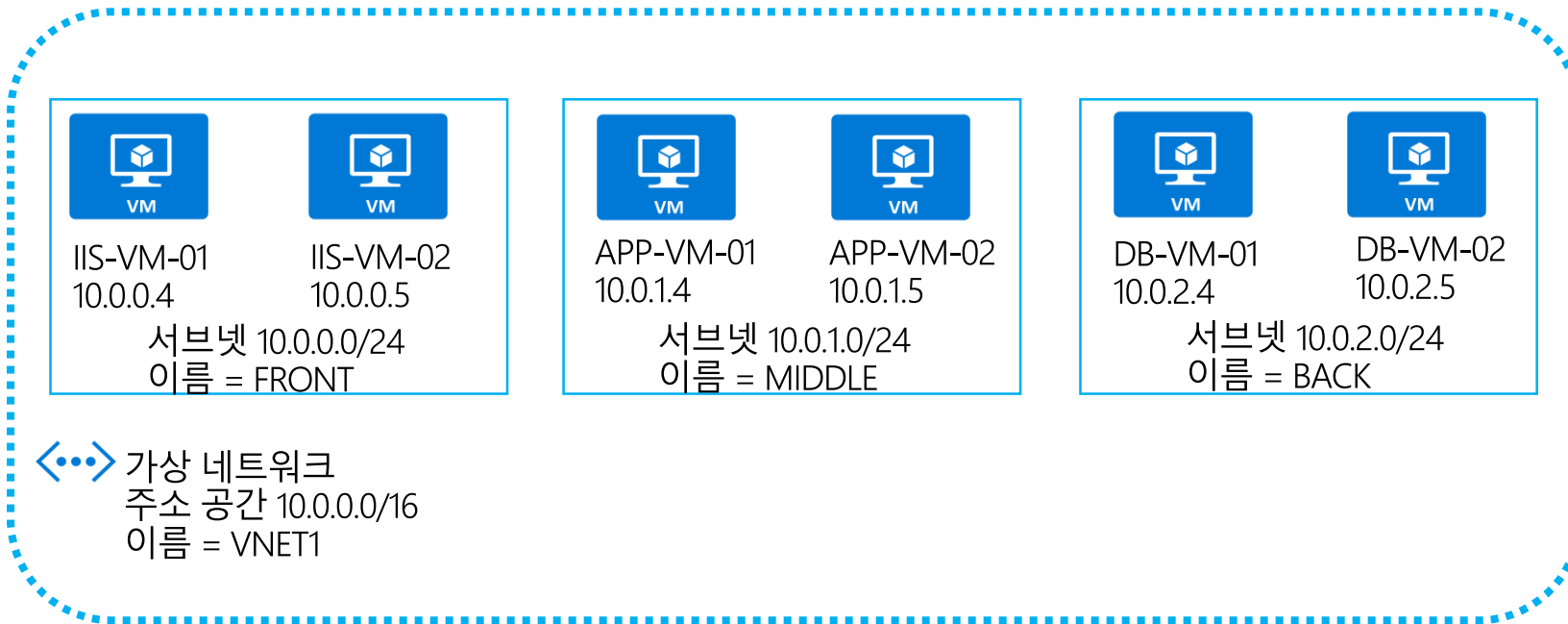


로드 밸런서 차이점

서비스	Azure 로드 밸런서	응용 프로그램 게이트웨이	트래픽 관리자
기술	전송 계층 (L4)	응용 프로그램 계층 (L7)	DNS 계층
지원되는 응용 프로그램 프로토콜	모두	HTTP 및 HTTPS	모두 (엔드포인트 모니터링에는 HTTP 엔드포인트가 필요)
엔드포인트	Azure VM 및 클라우드 서비스 역할 인스턴스	Azure 내부 IP 주소 또는 공용 인터넷 IP 주소	Azure VM, 클라우드 서비스, Azure 웹 응용 프로그램 및 외부 엔드포인트
VNet 지원	인터넷 연결 및 내부 응용 프로그램(VNet) 모두에 사용	인터넷 연결 및 내부 응용 프로그램(VNet) 모두에 사용	인터넷 연결 응용 프로그램만 지원
엔드포인트 모니터링	프로브를 통해 지원됨	프로브를 통해 지원됨	HTTP/HTTPS GET을 통해 지원됨

Virtual Network

3 tire app – vNet



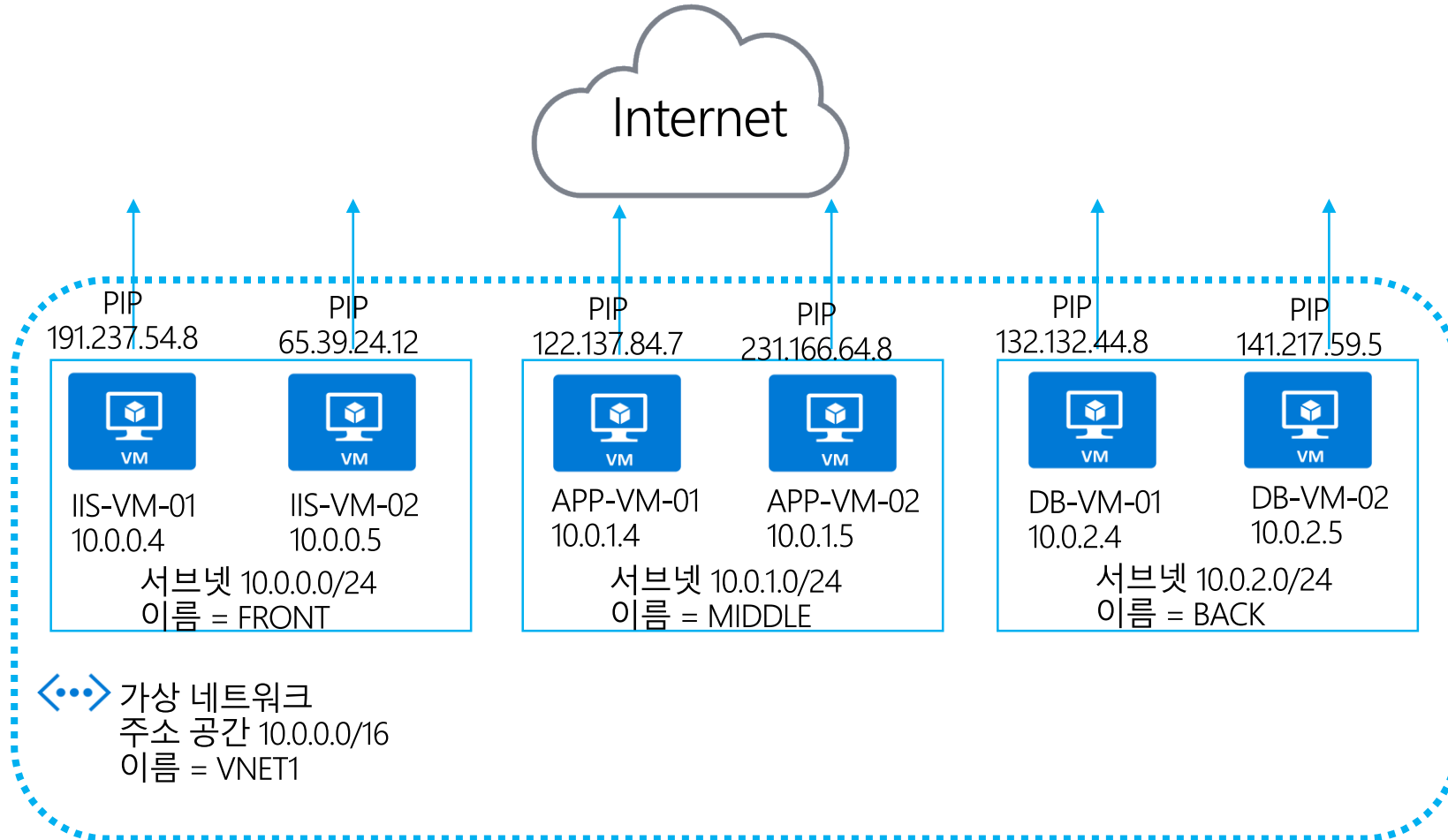
예측 가능하고 지속적인 IP 주소를 사용하여 클라우드에 개인 주소 공간을 선언

- RFC 1918 범위
- 고객이 등록한 IP 주소 범위

VNET 내의 서브넷은 완전히 라우팅 가능
가상 네트워크에 많은 주소 공간과 서브넷을 추가할 수 있음

Virtual Network

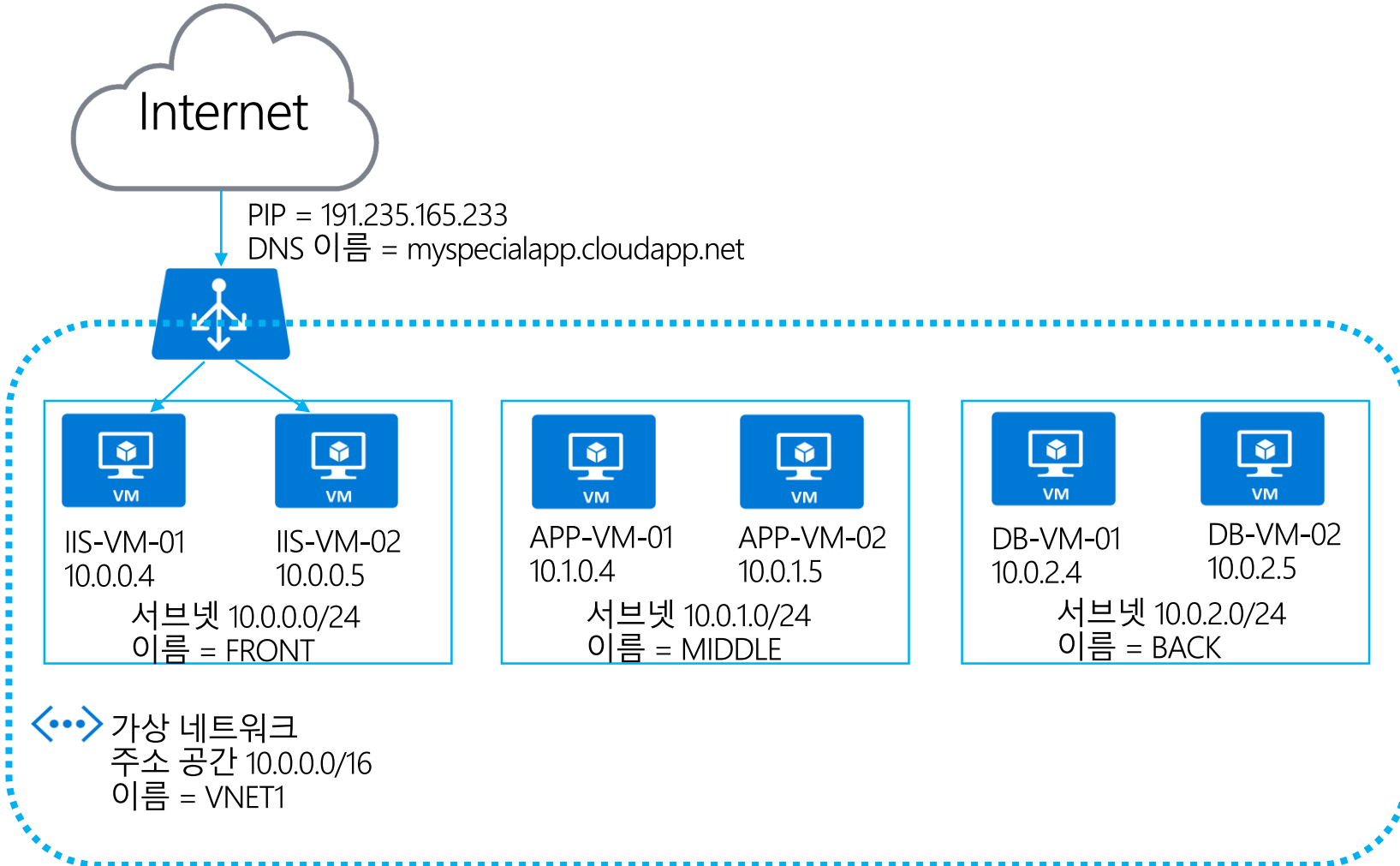
3 tire app – Internet access 가능한 기본 vNet



기억할 것: 공용 IP 주소는 Azure 개체이며 각 VM에 할당됨(실제 NIC 또한 Azure의 개체임). 이 디자인으로 모든 포트는 액세스할 수 있음!!

Virtual Network

vNet + LoadBalancer



웹 프론트 엔드를 Azure 로드 밸런서를 통해 인터넷에 게시

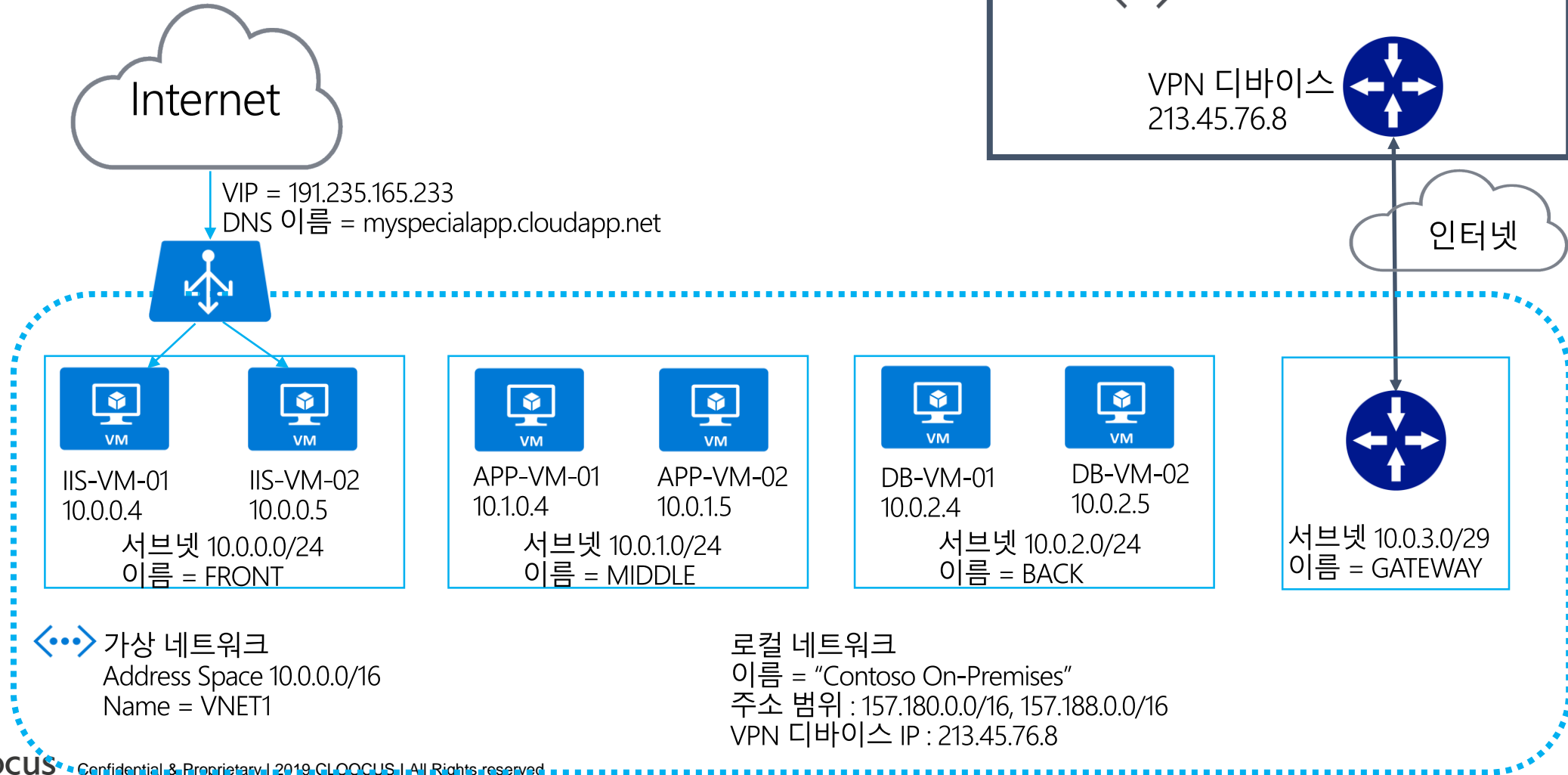
로드 밸런싱과 NAT 규칙 모두 지원

VIP 혹은 DNS 도메인 이름을 통해 액세스

Virtual Network

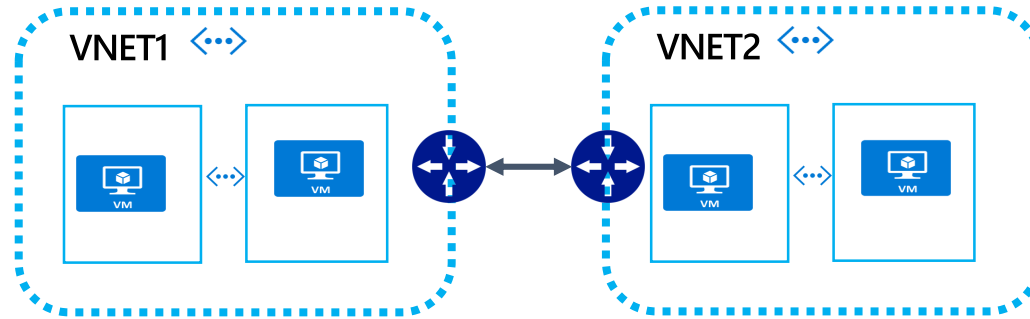
vNet + Internet access + on-premise 연결

Site-to-Site VPN / ExpressRoute를 통해



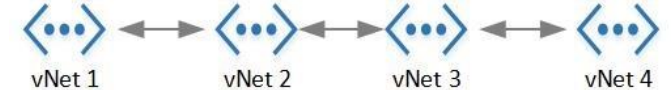
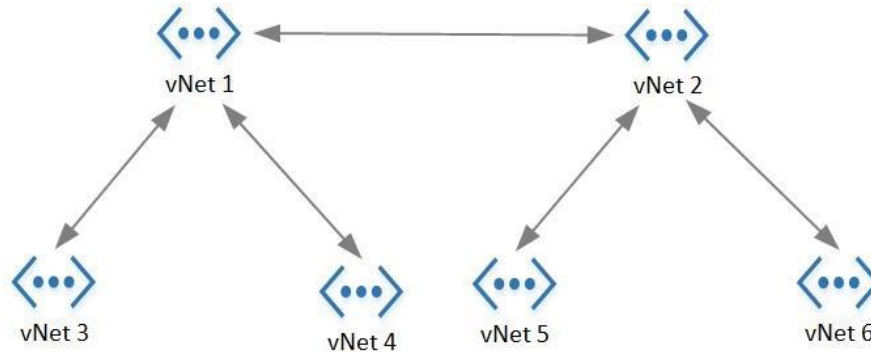
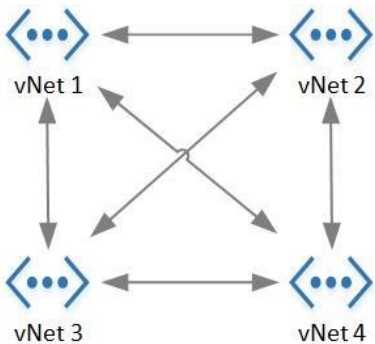
Virtual Network

vNet 간 Site-to-Site VPN 연결



제한 사항에 유의: 표준 VPN 게이트웨이에서 10 개 연결, 고성능에서 30 개 연결 제한 + 대역폭 제한

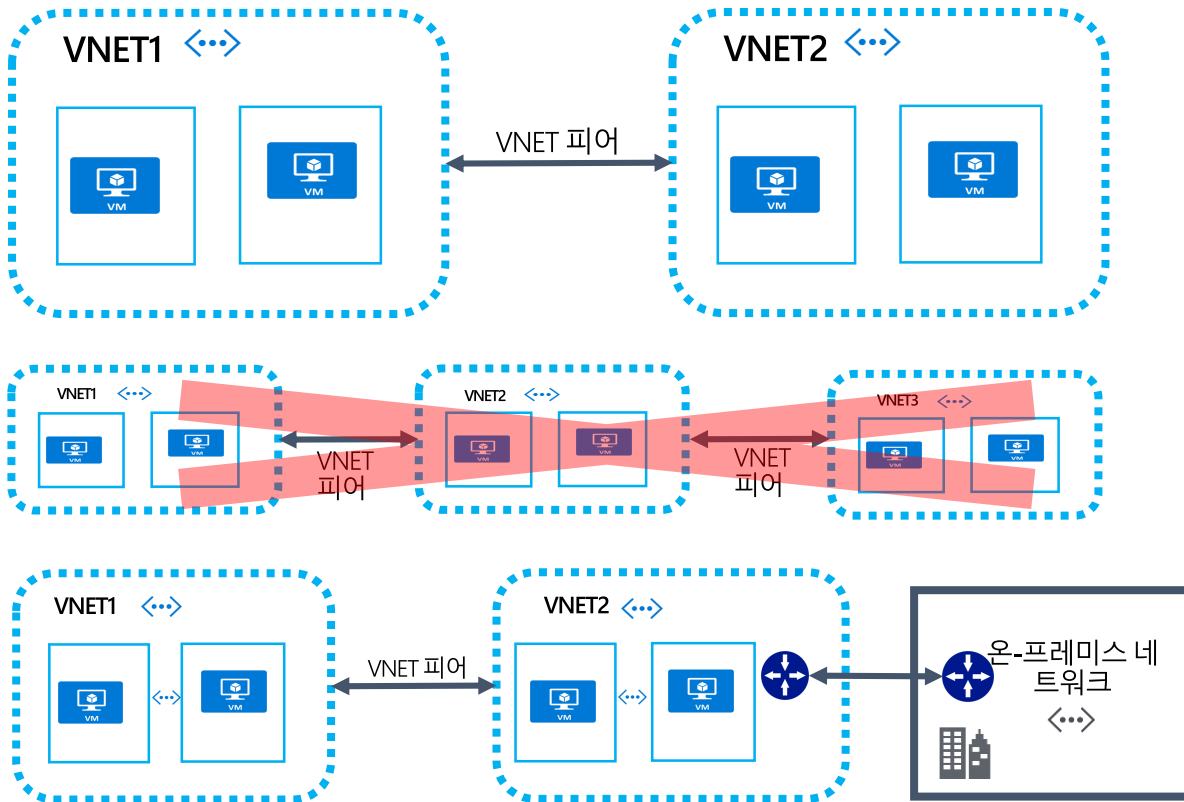
지역 내부 및 외부 연결 지원
아래와 같은 토폴로지를 지원:



ExpressRoute는 VNET 피어링을 활성화
(동일한 ER Circuit에 연결된 모든 VNET은 기본적으로 완전히 라우팅 됨. 따라서 VNET 간 S2S 연결을 설정할 필요가 없음)

Virtual Network

vNet Peering



VNet 피어링은 Azure 백본 네트워크를 통해 동일한 지역 및 다른 지역의 두 가상 네트워크를 연결하는 메커니즘
글로벌 VNet 피어링은 암호화 없이 서로 다른 두 지역간 연결이 가능
피어링된 가상 네트워크는 IP 주소가 겹치지 않아야 함

지원:

- VNET 에서 VNET
- 다른 구독에 있는 VNET 지원

게이트웨이가 필요하지 않음

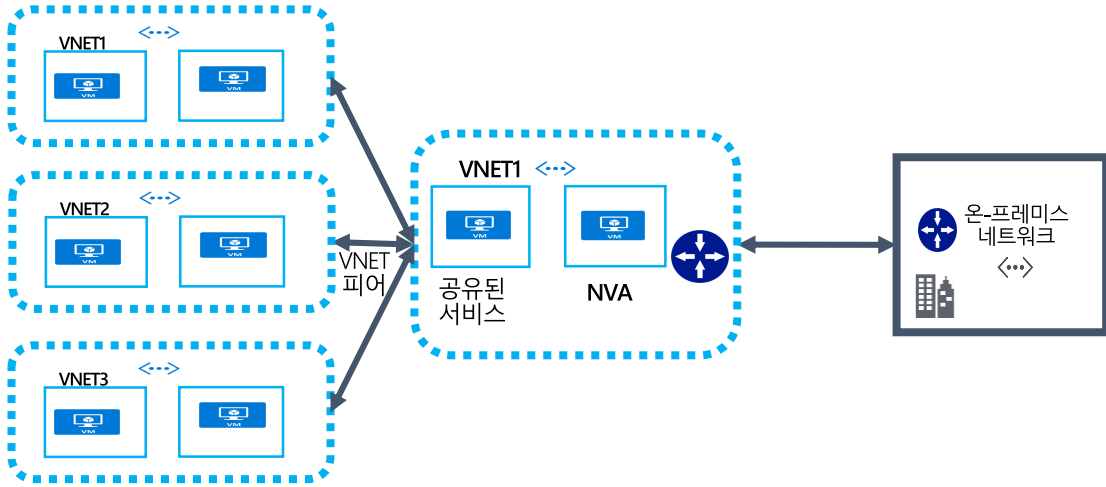
피어링의 **Transitivity**는 지원되지 않음

- VNET1에서 VNET2로 피어링을 구성하고 VNET2에서 VNET3으로 피어링을 구성한 것은 VNET1에서 VNET3으로 피어링을 구성한 것과 **다름**

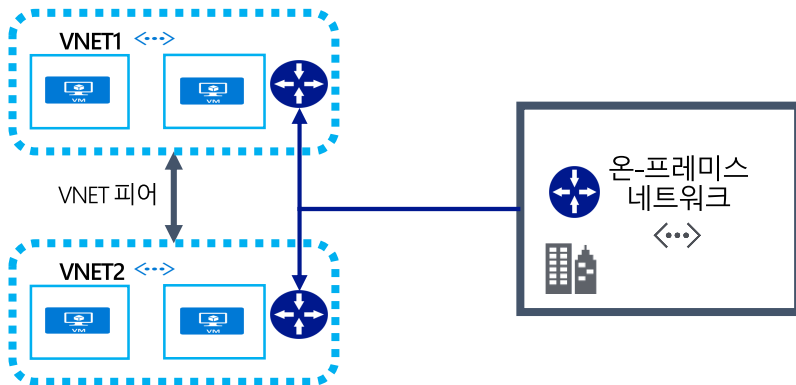
게이트웨이를 통한 온-프레미스로의 Transit은 지원됨
(UDR 포워딩 지원)

Virtual Network

vNet Peering

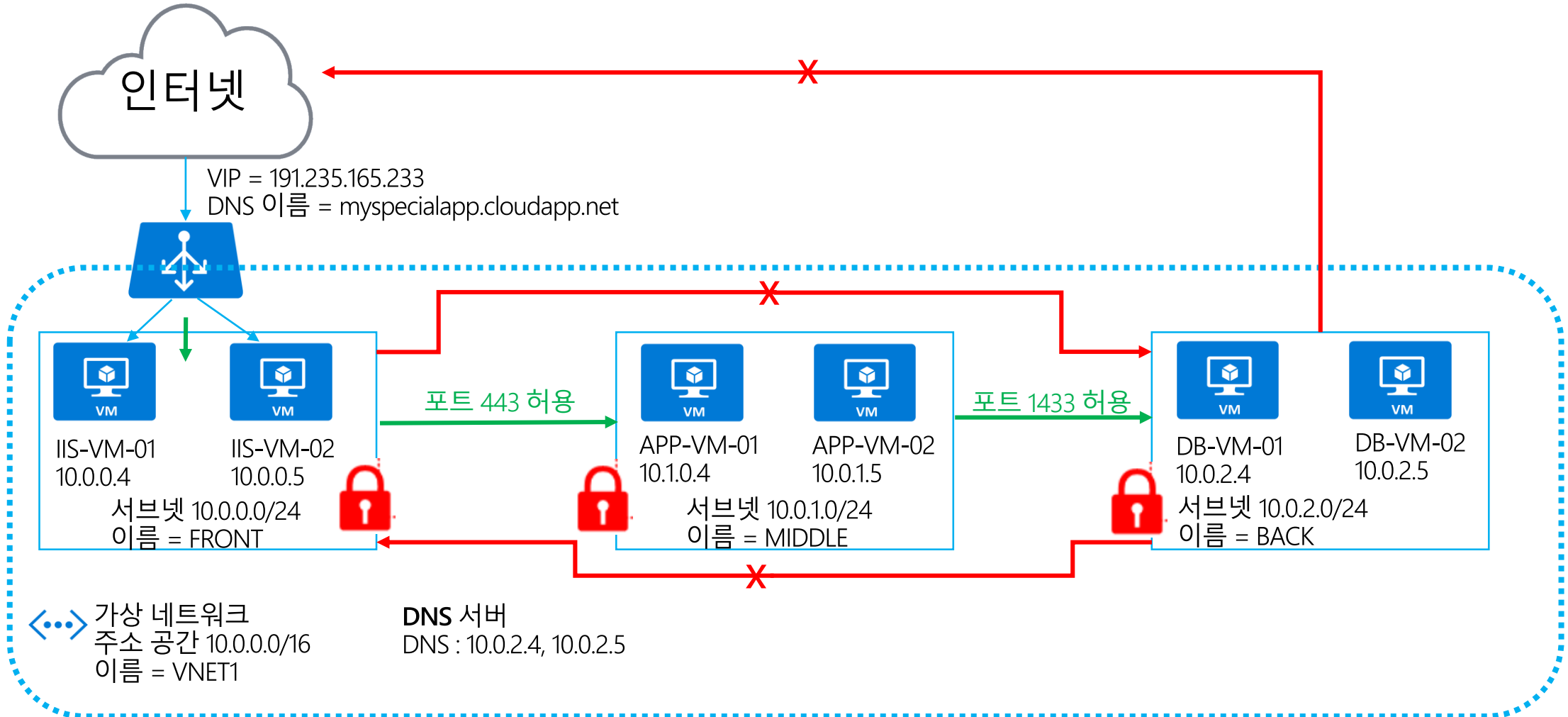


- Spoke VNET과 피어링 된 중앙 VNET 허브
- 게이트웨이 네트워크 가상 어플라이언스(NVA) transit 허용
 - 통합된 공유 서비스 지원



VNET 간 트래픽이 ER circuit을 선호하는 ExpressRoute 시나리오에서 유용함(POP를 통한 transit)

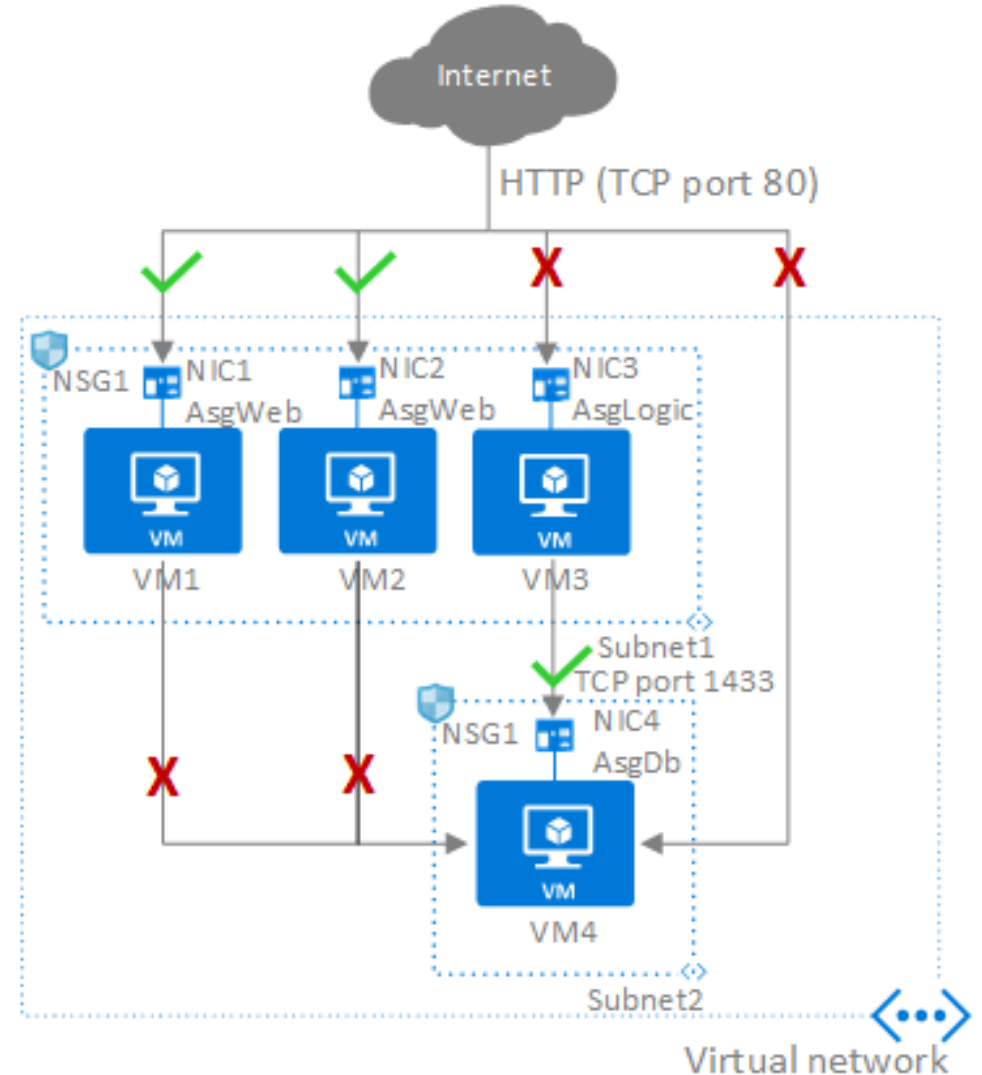
NSG(Network Security Group)



ASG(Application Security Group)

응용 프로그램 구조에 대한 네트워크 보안 구성
 가상 머신을 그룹화하고 보안 정책을 설정
 인바운드 및 아웃바운드 규칙
 우선 순위 기반 규칙

규칙	우선 순위	원본	원본 포트	대상	대상 포트	Protocol	Access
Allow-HTTP-Inbound-Internet	100	Internet	*	AsgWeb	80	TCP	Allow
Deny-Database-All	120	*	*	AsgDB	1433	All	Deny
Allow-Database-BusinessLogic	110	AsgLogic	*	AsgDB	1433	TCP	Allow





Thank you

Focus on Cloud

Microsoft Azure Consulting Expert Group

Cloocus
Beyond the Cloud

Gold
Microsoft
Partner
 Microsoft