

Microsoft Azure Fundamentals

AZ-900

1. Understand Cloud Concepts

1. Understand Cloud Concepts

클라우드의 정의

On-demand self-service

Ubiquitous network access

Location transparent resource pooling

Rapid elasticity

1. Understand Cloud Concepts

클라우드 서비스에는 아래와 같은 특성으로 정의 가능

High availability (HA) : The ability of the application to **continue running in a healthy state**, without significant downtime. By "healthy state," we mean the application is responsive, and users can connect to the application and interact with it.

Disaster recovery (DR) : The ability to recover from rare but major incidents: non-transient, wide-scale failures, such as service disruption that **affects an entire region**. Disaster recovery includes data backup and archiving, and may include manual intervention, such as restoring a database from backup.

Scalability : **Increase or decrease** the resources and services used based **on the demand or workload at any given time**.

Global reach : Cloud providers have fully-redundant datacenters located in **various regions all over the globe** (performance, redundancy, compliance).

Elasticity : **Automatically add or remove resources based on demand**.

Cloud Agility : Cloud agility is the ability **to rapidly change an IT infrastructure** in order to adapt to the evolving needs of the business (e.g. if your service peaks one month, you can scale to demand and pay a larger bill for the month. If the following month the demand drops, you can reduce the used resources and be charged less).

Cost Effective: Pay-as-you-go, consumption-based pricing model. Rather than paying for hardware up-front, you rent hardware and pay for the resources that you use.

Fault tolerance : Redundancy is often built into cloud services architecture so **if one component fails, a backup component takes its place**. This is referred to as fault tolerance and it ensures that your customers aren't impacted when an unexpected accident occurs.

Security : Cloud providers offer a broad set of policies, technologies, controls, and expert technical skills that can provide better security than most organizations can otherwise achieve.

1. Understand Cloud Concepts

Economies of Scale

규모의 경제로 운영하여 비용을 최소화할 수 있고 효율적으로 작업 수행할 수 있다. 클라우드 업체는 규모의 경제의 이점을 활용하여 그 혜택을 고객에게 돌려주는 것이 가능하다.

CapEx vs OpEx

Capital Expenditure (CapEx) :

물리적 인프라에 대한 지출을 선불로 지불하여 세금 계산서에서 비용을 공제한다. 높은 초기 비용, 투자 가치는 시간이 지남에 따라 감소한다.

Operational Expenditure (OpEx) :

필요에 따라 서비스 또는 제품에 지출되고 즉시 청구된다. 같은 해에 세금 계산서에서 비용을 공제한다. 선 결제 비용, 종량제 사용이 없다. MS의 Azure는 Public cloud이지만 Azure Stack이라고 하는 Private cloud 서비스도 지원한다. 클라우드를 사용할 경우 OpEx로 들어간다.

1. Understand Cloud Concepts

Public Cloud, Private Cloud, Hybrid Cloud 차이

Public Cloud

클라우드 서비스 또는 호스팅 공급자가 소유한다. 여러 조직과 사용자에게 리소스와 서비스를 제공한다.

보안 네트워크 연결을 통해 접근된다. (일반적으로 인터넷을 통해)

CapEx 없음 확장하기 위해 새 서버 구입 필요 없음.

민첩성 응용 프로그램에 빠르게 액세스할 수 있으며 필요할 때마다 프로비저닝을 해제할 수 있다. 소비 기반 모델이다.

Private Cloud

클라우드 리소스를 사용하는 조직이 소유 및 운영을 한다.

조직은 데이터센터에 클라우드 환경을 만든다.

조직 내의 사용자에게 제공되는 컴퓨팅 리소스에 대한 셀프 서비스 액세스

조직에게 본인들이 제공하는 서비스를 운영할 책임이 있다.

Hybrid Cloud

공용 및 사설 클라우드를 결합하여 응용 프로그램이 가장 적절한 위치에서 실행되도록 한다.

1. Understand Cloud Concepts

IaaS = Servers and storage + Networking firewalls/Security + Datacenter physical plant/building

대부분 기본 클라우드 컴퓨팅 서비스 범주. 클라우드 공급자의 서버, 가상 머신, 스토리지, 네트워크 및 운영 체제를 대여하여 종량제 IT 인프라를 구축. 인터넷을 통해 프로비저닝 및 관리되는 인스턴트 컴퓨팅 인프라. 호스팅 서비스가 예시.

PaaS = Development tools, database management, business analytics + Operating systems + Servers + IaaS

소프트웨어 응용 프로그램을 빌드, 테스트 및 배포하기 위한 환경을 제공. 기본 인프라 관리에 집중하지 않고도 응용 프로그램을 신속하게 만들 수 있도록 지원. 개발.

SaaS = Hosted applications/apps + PaaS

최종 사용자를 위해 중앙에서 호스팅 되고 관리되는 소프트웨어. 사용자는 인터넷을 통해 클라우드 기반 앱에 연결하고 사용. 예를 들어 Microsoft Office 365, 전자 메일 및 일정 등. 일반 사용자의 소비.



SaaS

PaaS

IaaS



호스팅된
응용 프로그램/앱



개발 도구, 데이터베이스
관리, 비즈니스 분석



운영 체제



서버 및 저장소



네트워크
방화벽/보안



데이터 센터
물리적 공간/건물

1. Understand Cloud Concepts

	Basic	Developer	Standard	Professional Direct	Premier
Scope	Available to all Microsoft Azure accounts	Microsoft Azure: Trial and non-production environments	Microsoft Azure: Production workload environments	Microsoft Azure: Business-critical dependence	All Microsoft Products, including Azure: Substantial dependence across multiple products
Customer Service, Self-Help and Communities	24x7 access to billing and subscription support, online self-help, documentation, whitepapers, and support forums				
Best Practices	Access to full set of Azure Advisor recommendations				
Health Status and Notifications	Access to personalized Service Health Dashboard & Health API				
Technical Support	Not available	Business hours access ¹ to Support Engineers via email	24x7 access to Support Engineers via email and phone		
Third-Party Software Support	Not available	Interoperability & configuration guidance and troubleshooting			
Case Severity/Response Times	Not available	Minimal business impact (Sev C): <8 business hours ¹	Minimal business impact (Sev C): <8 business hours ¹ Moderate business impact (Sev B): <4 hours Critical business impact (Sev A): <1 hour	Minimal business impact (Sev C): <4 business hours ¹ Moderate business impact (Sev B): <2 hours Critical business impact (Sev A): <1 hour	Minimal business impact (Sev C): <4 business hours ¹ Moderate business impact (Sev B): <2 hours Critical business impact (Sev A): <1 hour <15 minutes (with Azure Rapid Response or Azure Event Management)
Architecture Support	Not available	General guidance		Architectural guidance based on best practice delivered by ProDirect Delivery Manager	Customer specific architectural support such as design reviews, performance tuning, configuration and implementation assistance delivered by Microsoft Azure technical specialists.
Operations Support	Not available			Onboarding services, service reviews, Azure Advisor consultations	Technical account manager-led service reviews and reporting

1. Understand Cloud Concepts

Azure community support

Channel	Description
Azure Knowledge Center	The Azure Knowledge Center is a searchable database that contains answers to common support questions.
Microsoft Tech Community	Get support by reading responses to Azure technical questions from Microsoft's developers and testers.
Stack Overflow	You can review answers to questions from the development community.
Server Fault	Review community responses to questions about System and Network Administration in Azure.
Azure Feedback Forums	Read ideas and suggestions for improving Azure made by Azure users.
Twitter	Tweet @AzureSupport to get answers and support from the official Microsoft Azure Twitter channel.

1. Understand Cloud Concepts

Azure Service Level Agreement (SLAs)

<https://azure.microsoft.com/en-us/support/legal/sla/summary/>

SLA는 서비스 또는 제품에 대한 약속

각 제품 및 서비스에 대해 개별 설정할 수 있다

SLA 3가지 구성 요소

Performance targets, uptime, connectivity 보장 : Uptime 혹은 availability

Performance targets 범위 : 보통 99.9% (three nines) 에서 99.99% (four nines)

Service Credit : SLA 보장을 맞추지 못한 경우 지원되는 월 서비스 비용

1. Understand Cloud Concepts

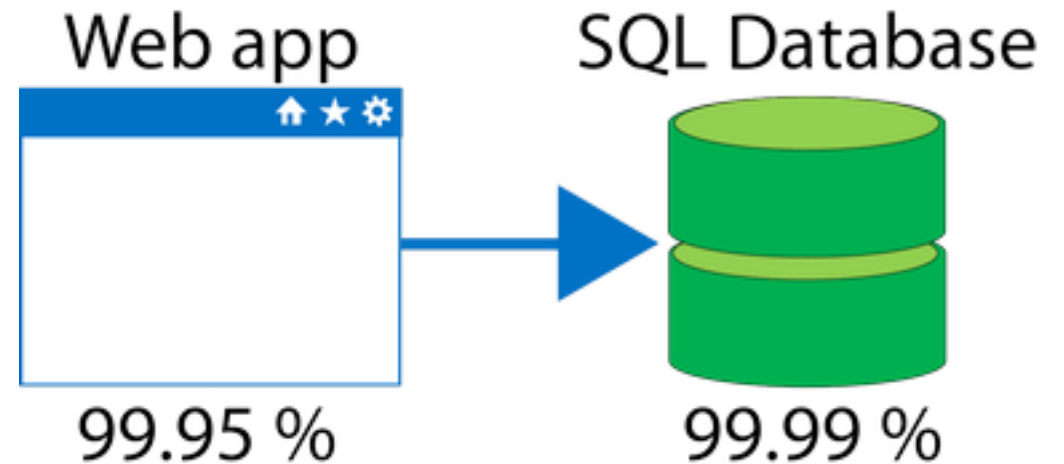
Composite SLAs

App Service web app에서 Azure SQL Database를 사용하는 솔루션의 경우 각각의 서비스는 아래와 같은 SLA를 제공

App Service Web Apps : 99.95%

SQL Database : 99.99%

두가지를 함께 사용할 때는 정확한 수치를 계산할 때는 두 수치를 곱해야 한다.
($99.95\% \times 99.99\% = 99.94\%$)



1. Understand Cloud Concepts

Service Life cycle

Azure Preview를 사용하면 베타 및 기타 시험판 기능, 제품, 서비스, 소프트웨어 및 지역을 테스트할 수 있다. Preview 는 두가지 종류가 있다.

Private Preview : available to * specific* Azure customers for evaluation purposes. This is typically by invite only and issued directly by the product team responsible for the feature or service.

Public Preview : available to all Azure customers for evaluation purposes. These previews can be turned on through the preview features page

Production 환경에서 사용 가능. SLA 적용 안됨.

General Availability (GA) : Once a feature has been evaluated and tested successfully, it might be released to customers as part of Azure's default product set.








1. Understand Cloud Concepts

Azure Migrate

Azure Migrate and Azure tooling is available free of charge.

However, you may incur charges if you choose to use ISV tools for additional capabilities.

마이그레이션 비용은 기본적으로 무료이나 ISV (Independent Software Vendor) 서비스 사용 시 유료

SCENARIO	TOOL	PROVIDER	PRICING
Servers	Server Assessment	Microsoft	Free ¹
	Server Migration	Microsoft	Free ²
		ISV	Learn more
		ISV	Learn more
		ISV	Learn more
		ISV	Learn more
		ISV	Learn more
		ISV	Learn more
Databases		ISV	Learn more
	Data Migration Assistant	Microsoft	Free
	Database Migration Service	Microsoft	Free ³
Web apps	App Service Migration Assistant	Microsoft	Free
Data	Data Box	Microsoft	Learn more

2. Understand Core Azure Services

2. Understand Core Azure Services

Region : 여러 데이터센터들이 위치한 지역

한 region의 여러 데이터센터들은 latency를 줄이기 위해 지리적으로 서로 가까운 곳에 위치한다.

Central US, East US 2, West US 2, West Europe, France Central, North Europe, Southeast Asia
Deploying an app can be done directly to **Region**

Azure special regions

특정 규정 준수 또는 법적 요구 사항이 있는 응용 프로그램.

Azure 정부(북미) : 미국 정부 전용 데이터센터

Azure 중국 : 21Vianet이라는 수탁업체와 함께 서비스를 제공한다.

Azure 독일 : 법적 이유로

2. Understand Core Azure Services

Geographies > Region pair > Data center > Availability zone

Geographies

데이터 상주(Residency) 및 규정(Compliance) 준수 경계를 보존하는 개별 시장.

Americas, Europe, Middle East and Africa, Asia Pacific --> 4개

Region pairs

각 Azure 지역은 동일한 지역 내에서 다른 지역과 Paring. Paring은 Azure 리소스를 복제하여 자연 재해, 전원 또는 네트워크 중단으로 인한 피해를 최소화 할 수 있다.

Geography	Paired regions	
Asia	East Asia	Southeast Asia
China	China North	China East
Europe	North Europe (Ireland)	West Europe (Netherlands)
Korea	Korea Central	Korea South
North America	East US	West US

AZURE GLOBAL INFRASTRUCTURE

GEOGRAPHIES Americas, Europe, Middle East and Africa, Asia Pacific

REGIONAL PAIRS East Asia – Southeast Asia pair

REGIONS East US, West US, Central India, South India

AVAILABILITY ZONES Availability Zone #1, #2, #3, #4

DATACENTERS

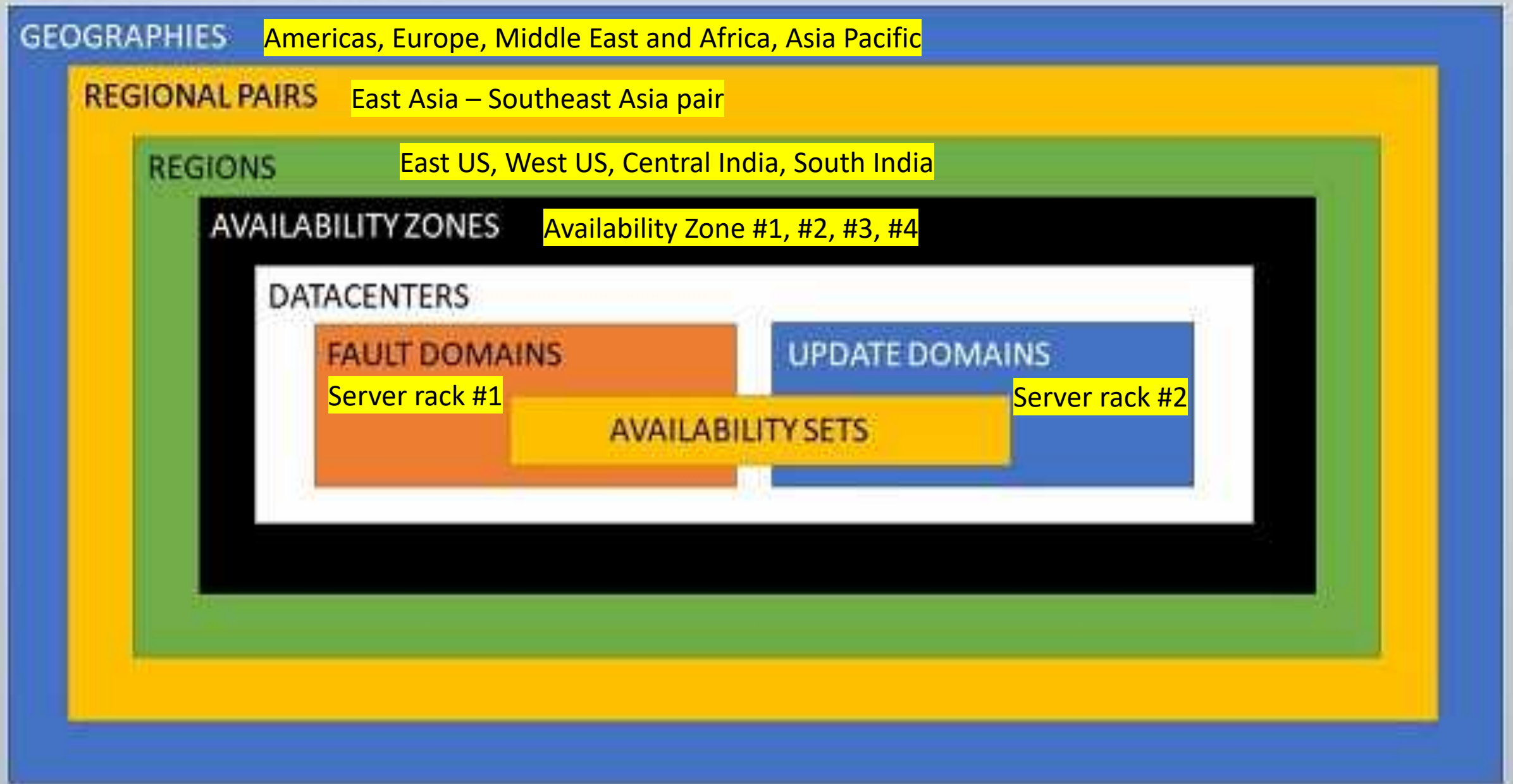
FAULT DOMAINS

Server rack #1

UPDATE DOMAINS

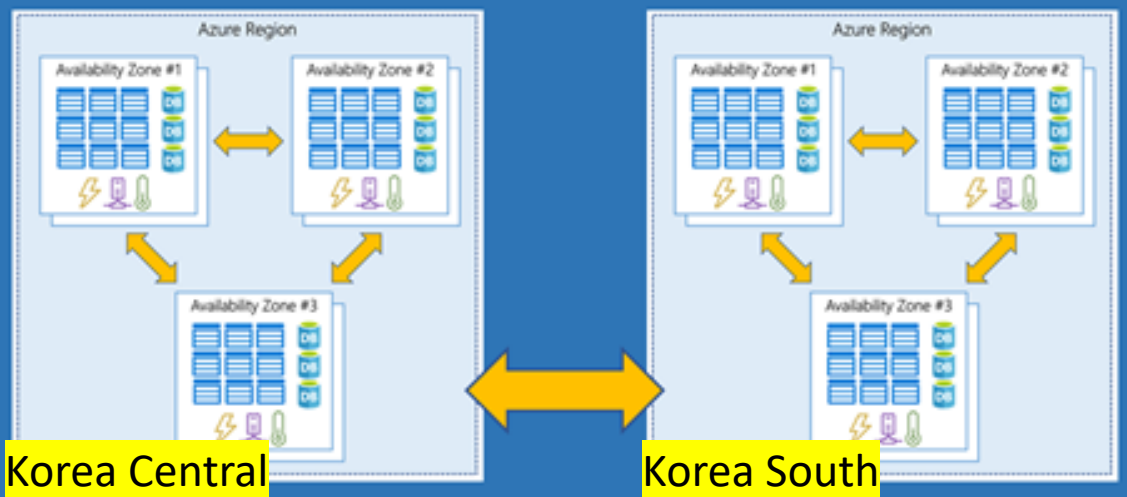
Server rack #2

AVAILABILITY SETS

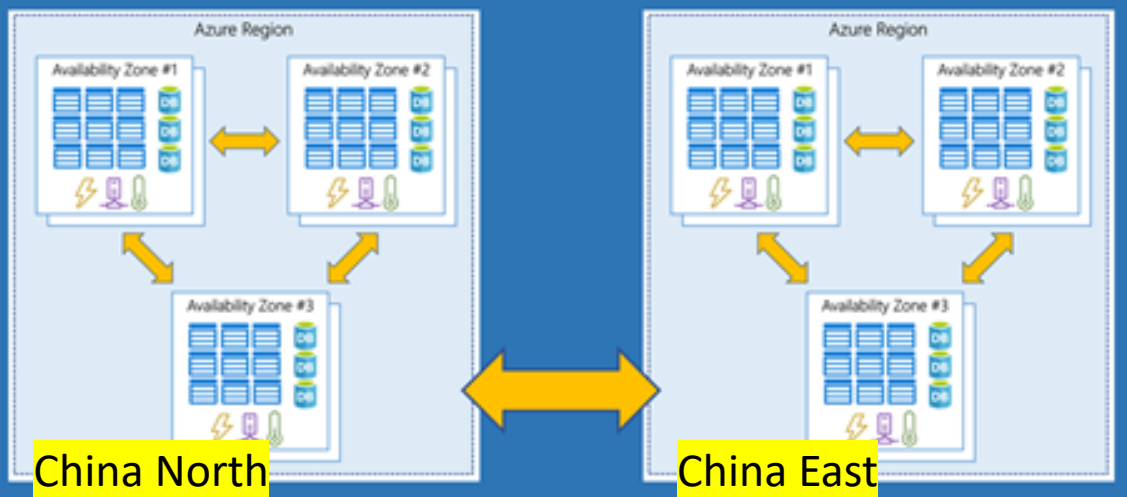


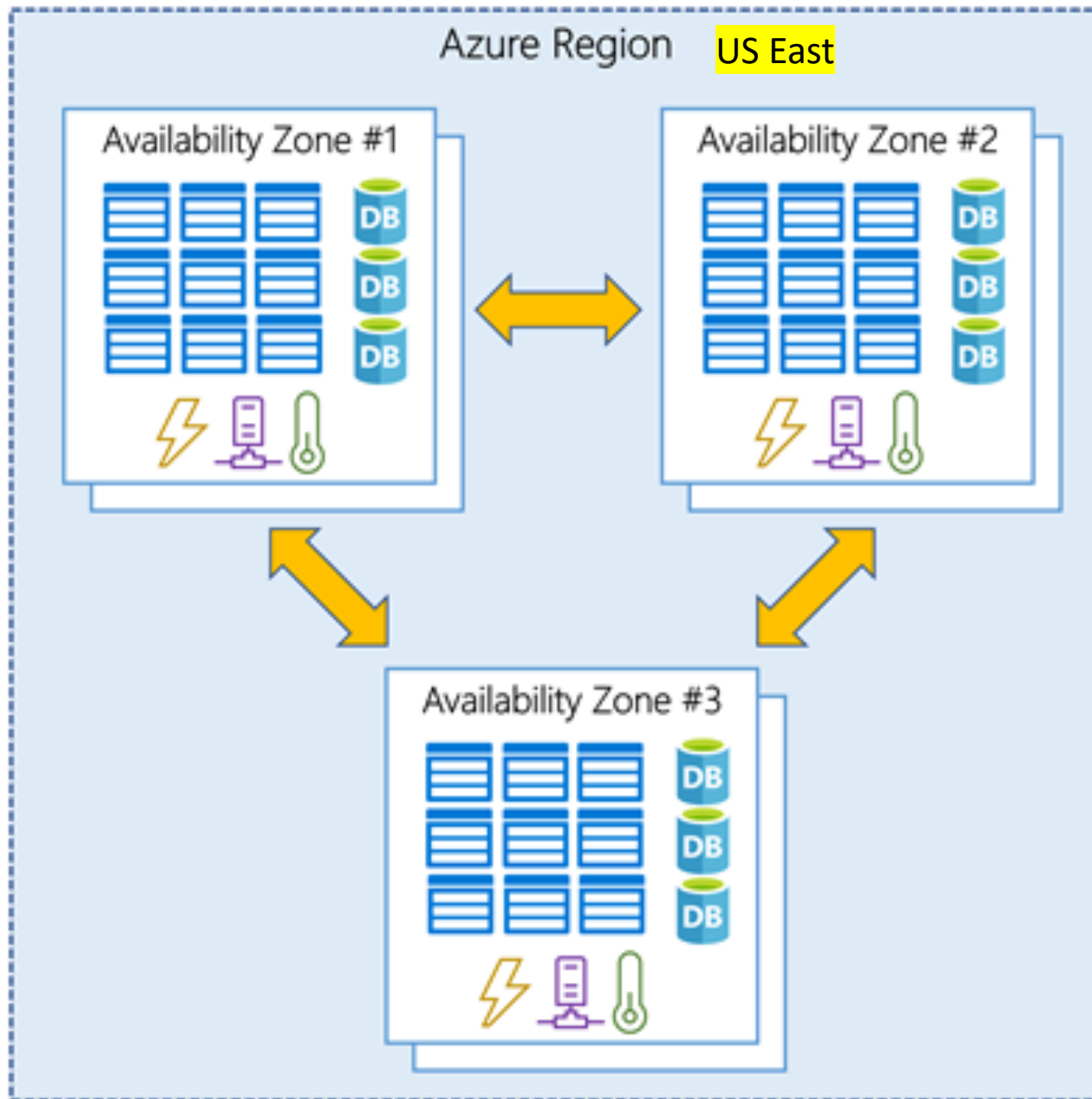
Geography Asia Pacific

Region Pair Korea





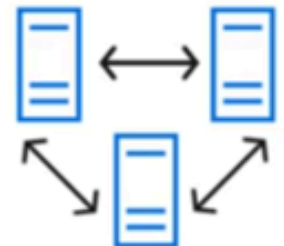
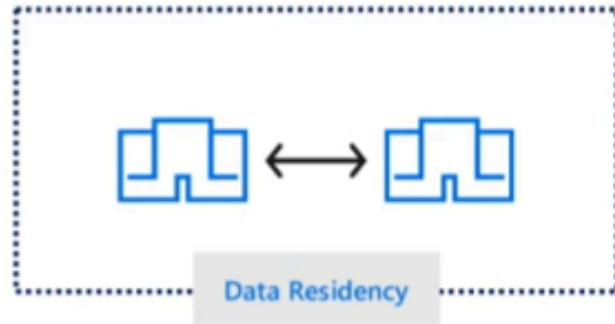
Region Pair China





Separate building in a same region

가용성 옵션

VM SLA 99.9% 프리미엄 저장소 사용	VM SLA 99.95%	VM SLA 99.99%	MULTI-REGION DISASTER RECOVERY
			
단일 VM lift and shift	Availability Set 데이터센터 내 장애 방지	Availability Zone 데이터센터 간 장애 방지	지역 쌍 (REGION PAIRS) 지역간 장애 방지

2. Understand Core Azure Services

Availability Zones

Availability Set의 개념을 동일 Region내에 물리적으로 분리된 장소(데이터센터)로 확장한 개념. Protect apps and data from datacenter outages and maintenance events.

Physically separate locations within an Azure region. Each Availability Zone is made up of one or more datacenters equipped with independent power, cooling, and networking. Availability Zones allow customers to run mission-critical applications with high availability and low-latency replication.

모든 region에서 지원하는 것은 아니다.

SLA

Region > Resource Group > Single instance VM, VMs in Availability set, Scale sets

2. Understand Core Azure Services

Availability sets

유지 관리 또는 하드웨어 오류 발생 시 응용 프로그램을 온라인 상태로 유지

To provide redundancy to application, group two or more VM in an availability set.

It ensures that during a planned or unplanned maintenance event, at least one VM will be available and meet the 99.95% SLA. The availability set of a virtual machine can't be changed after it is created.

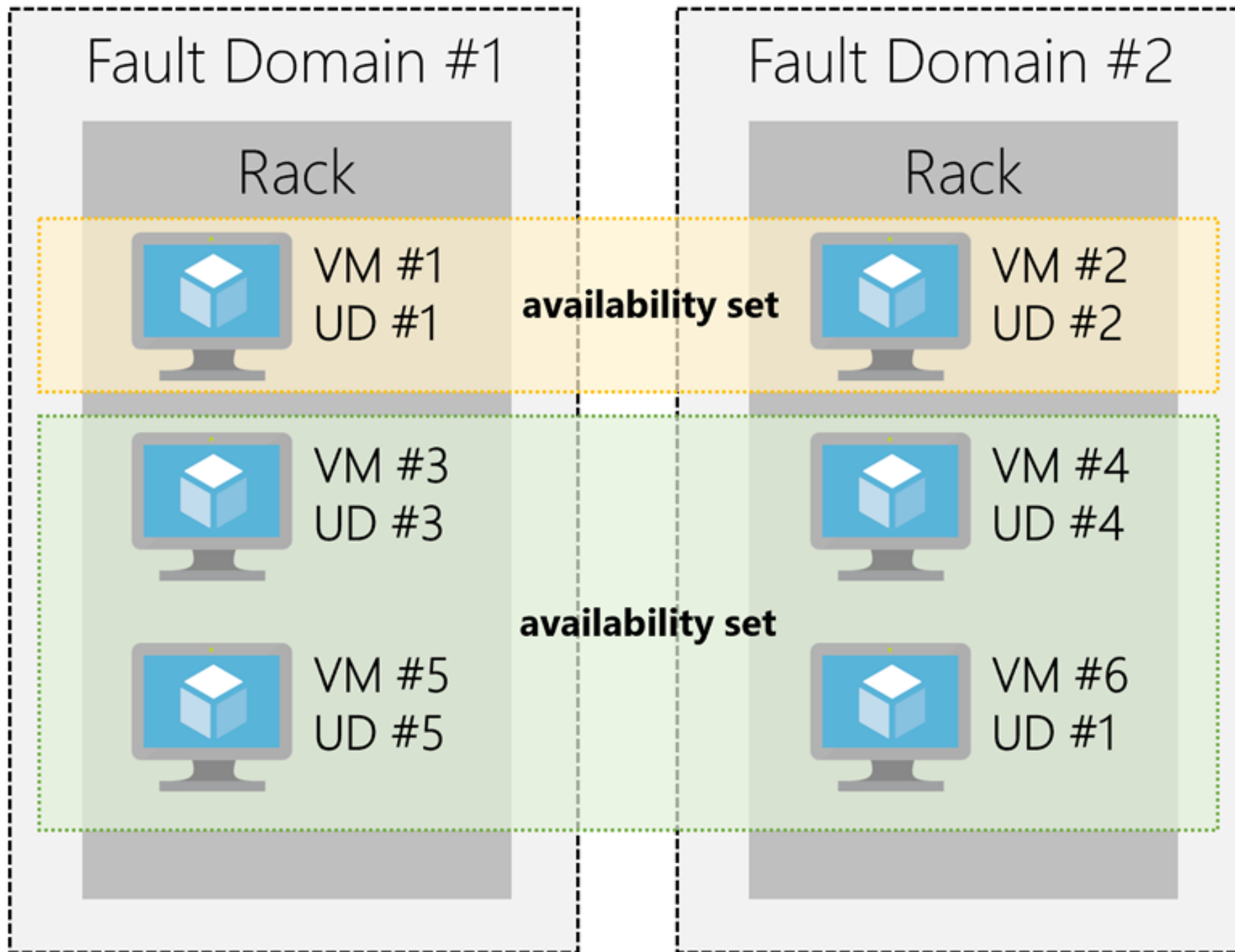
구성

Fault domains (FD) : Virtual machines that share a fault domain have a common power source and network switch.

Update domains (UD) : Virtual machines that share an update domain can undergo maintenance or be rebooted at the same time. 예약된 유지 관리, 성능 또는 보안 업데이트는 업데이트 도메인을 통해 순서가 정해진다. 패치, 보안 업데이트를 한번에 동시에 할 수 있게 하도록 고안된 단위.

* MS는 사용자가 싱글 리소스만 사용할 경우 Fail시 SLA를 적용되지 않는다. Availability sets를 만들어서 VM 한 개 이상의 리소스를 넣어야 한다.

* Region별로 서비스를 복수(예를 들어 한국과 영국 Region) 운영하는 것은 각 국가별 사용자를 위해 각각 운영하는 것이고 High availability을 위한 작업은 Availability sets 기능을 사용해야 한다.



Fault Domain =
Separated server racks

VM in the same fault
domain share a common
power source and physical
network switch

2. Understand Core Azure Services

Azure subscriptions

Azure Subscriptions (Unit of Azure products and services)

<--- Authentication & Authorization --->

Azure account (Identity in Azure AD or trusted directory)

2. Understand Core Azure Services

Subscription 관리

Billing : 과금 리포트 및 비용 정산이 월별 subscription 단위로 진행

Access Control : subscription은 Azure 리소스에 대한 배포 경계로 역할 기반 액세스 제어(RBAC)를 설정할 수 있는 기능

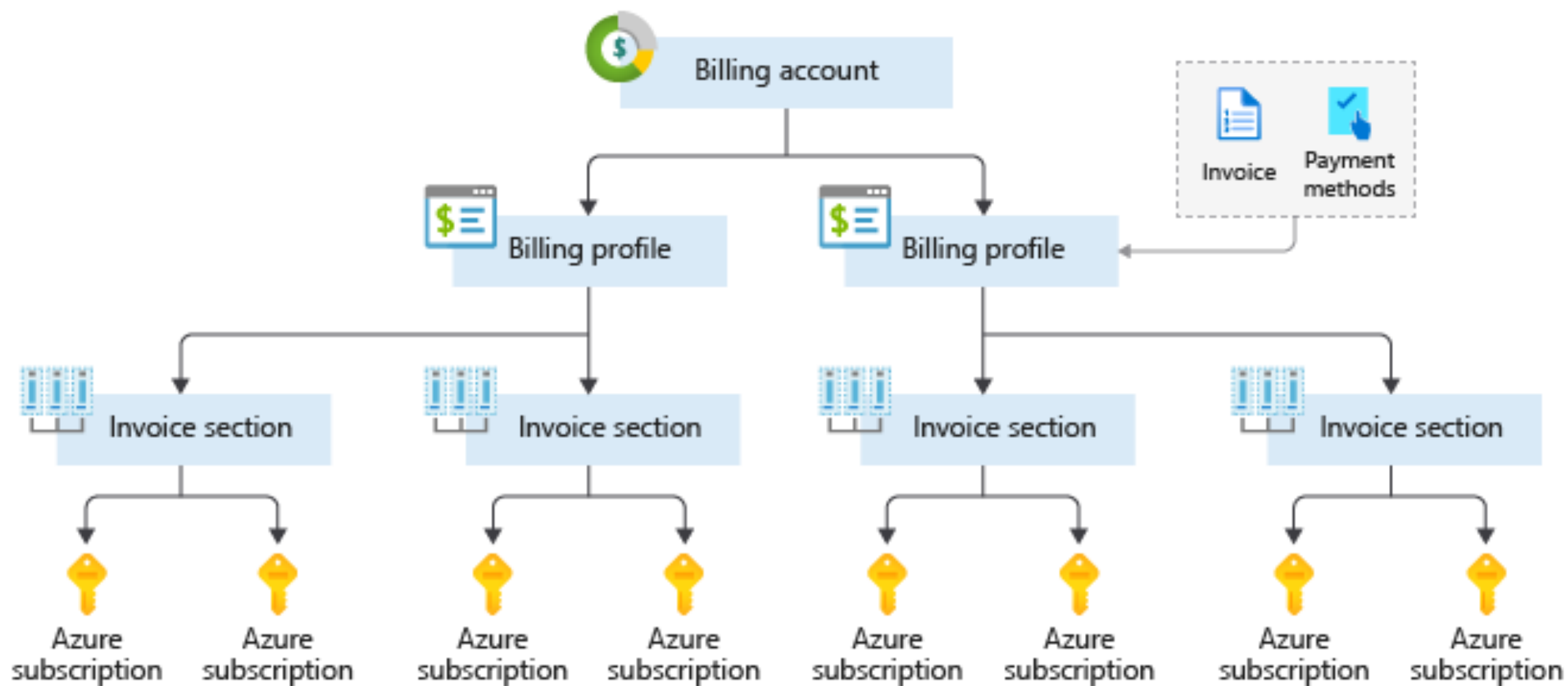
Subscription Limits : subscription 기반으로 주어진 Hard Limit이 존재. 특정 시나리오에서 이러한 제한을 초과해야하는 경우 추가 subscription 생성이 필요할 수 있음. If you hit a hard limit, there is no flexibility. 스타트업 같은 경우는 하나의 subscription만 사용해도 되지만 부서 별로 비용이 다르게 배분되는 경우 여러개의 subscription을 따로 만들어서 관리할 수 있다.

Subscription 을 사용하는 이유

Billing boundary : 과금 경계를 정하기 위해

Access control boundary : 액세스 접근 제안의 경계를 정하기 위해

Azure Resource Manager : 리소스 그룹 및 리소스 그룹 내의 모든 리소스가 생성, 구성, 관리 및 삭제되는 관리 계층을 제공



2. Understand Core Azure Services

Azure Resource Manager

provide a common platform for deploying objects to a cloud infrastructure and for implementing consistency across the Azure environment.

Deploy app resources together and easily repeat deployment tasks

repeatedly deploy your app, deployed in a consistent state

Organize resources to clarify billing and management

manage and visualize resources in your app, put resources with a common lifecycle into a resource group, see which resources are linked by a dependency, apply tags

Control access to resources

manage permissions by defining roles and adding users or groups to the roles, apply an explicit lock, logs all user actions so you can audit those actions

2. Understand Core Azure Services

Azure Object Hierarchy : 리소스들은 논리적으로 4레벨을 가짐

Management groups > Subscriptions > Resource groups > Resources

Management groups

Azure 관리 그룹은 여러 Azure subscription에서 액세스, 정책 및 규정 준수를 관리하기 위한 컨테이너.

관리 그룹을 사용하면 Azure 리소스를 계층적으로 컬렉션으로 정렬할 수 있게 하기 때문에 subscription을 넘어 더 높은 수준의 분류를 제공할 수 있음.

2. Understand Core Azure Services

Resource Groups

응용 프로그램에서 요구하는 리소스를 관리 가능한 단일 단위로 집계하는 컨테이너 역할.

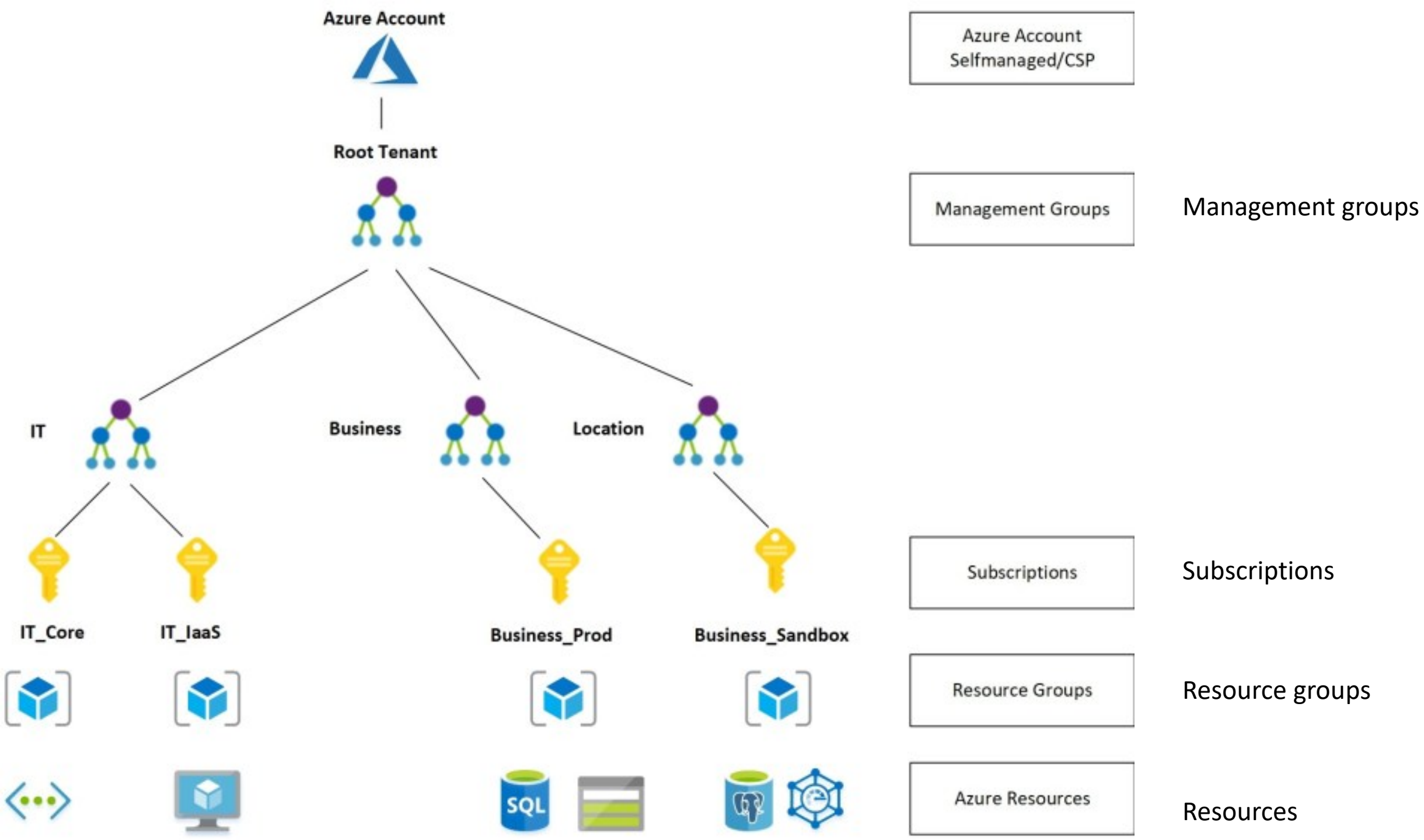
모든 Azure 리소스는 하나의 리소스 그룹에만 존재.

RBAC을 통해 리소스 권한 관리.

서비스 별로 무조건 리소스 그룹을 만드는게 좋다.

리소스는 리소스 그룹 간에 이동이 가능하다

* RBAC : 파일시스템의 Permission과 비슷한 개념



2. Understand Core Azure Services

Azure Compute service

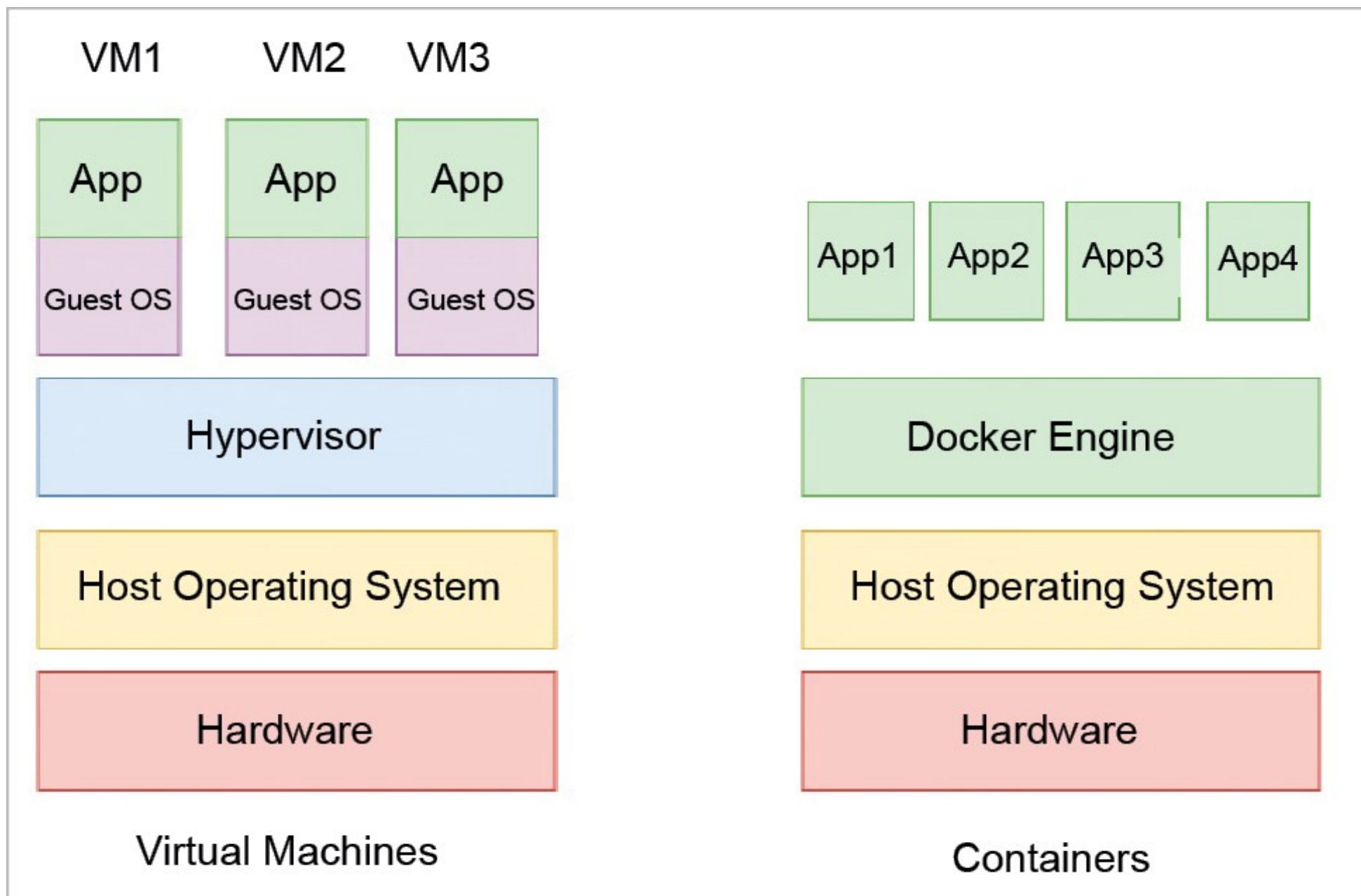
Container services

컨테이너는 가상 환경이다. 그러나 VM처럼 개별적인 OS위에서 돌아가는게 아니라 현재 돌아가는 호스트 OS 에서 여러 컨테이너들이 해당 OS를 함께 사용한다. 컨테이너는 경량(lightweight)이어야 하며 동적으로 생성, 확장 및 중지되도록 설계됨

컨테이너에 대한 Azure 서비스의 예

Azure container instances : 컨테이너 업로드 후 **빠르고 쉽게 돌릴 수 있는 PaaS 환경**

Azure Kubernetes Service (AKS) : **대량의 컨테이너**를 자동화, 관리, 상호작용 (Orchestration) 할 수 있음



2. Understand Core Azure Services

Scale Set

Create and manage a group of identical, load balanced VMs. PaaS

Allow you to centrally manage, configure, and update a large number of VMs in minutes to provide highly available applications

The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. VM inside a scale set can be deployed into fault domains or Availability zones.

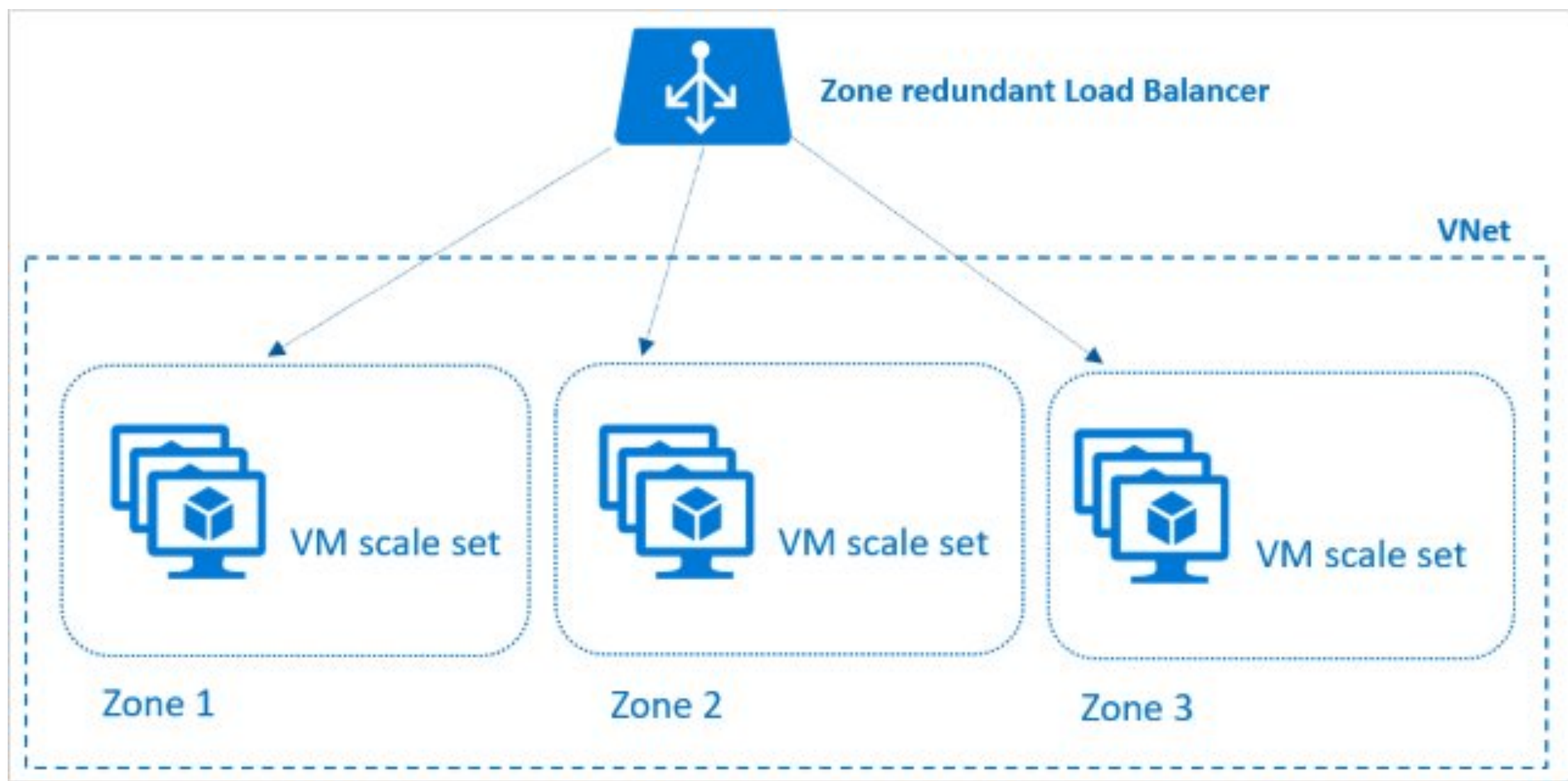
Scale set must be set to VM orchestration mode, and the same region and resource group.

Integrated with Azure Autoscale and Azure Load Balancer

Availability Set 과 Scale Set 의 차이

Availability Set : Redundancy. 한 VM 실패 시 다른 VM이 작동됨

Scale Set : 사용자 요구 수준에 따라 자동으로 VM 수가 증가/축소 됨

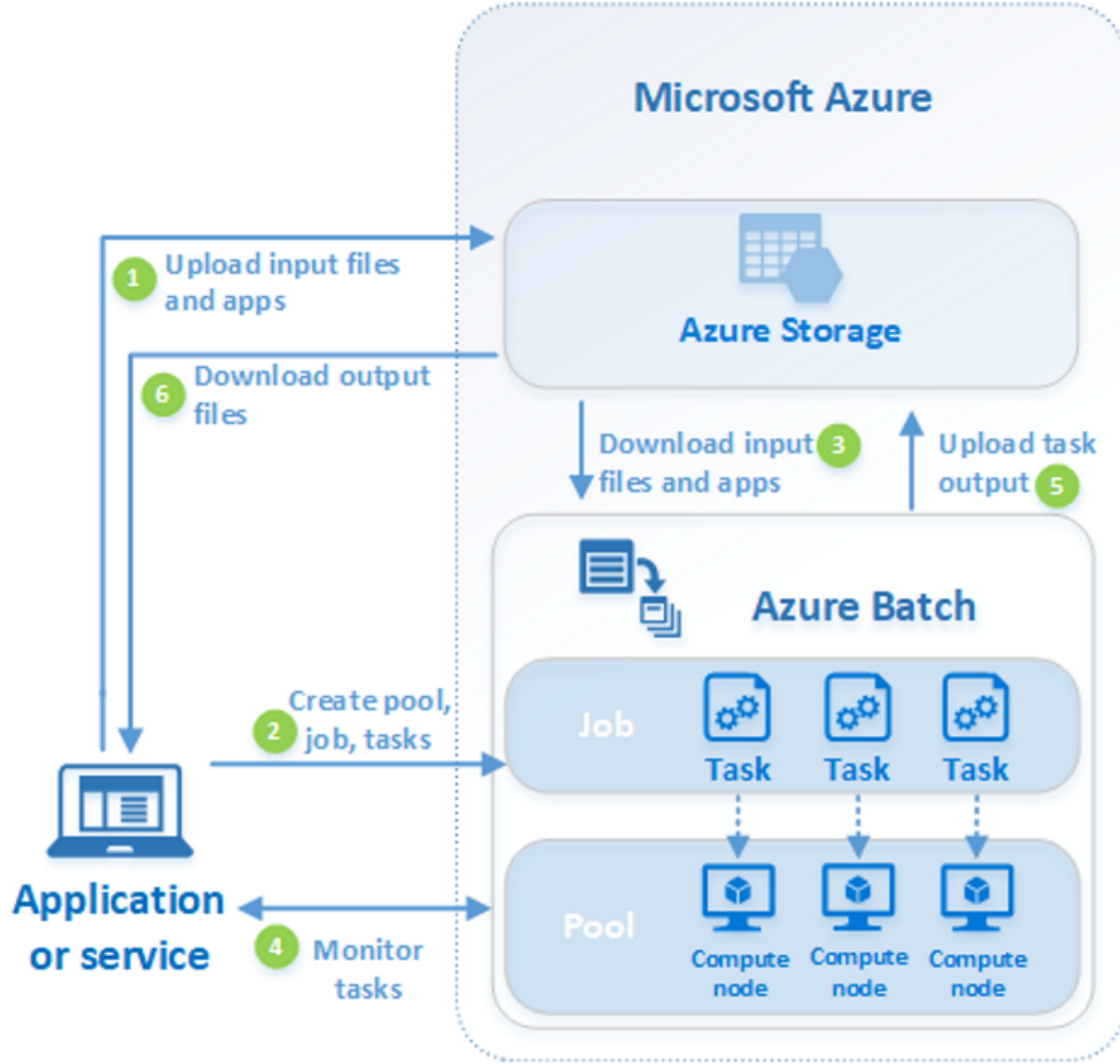


2. Understand Core Azure Services

Azure Batch

Enables large-scale job scheduling and compute management with the ability to scale to tens, hundreds, or thousands of VMs.

There may be situations in which you need raw computing power or supercomputer level compute power. Azure provides these capabilities.



2. Understand Core Azure Services

Serverless computing

Azure Functions : 서비스를 위한 코드에 집중. 인프라 및 플랫폼으로부터의 자유도 확보

Azure Logic Apps : 작업 및 비즈니스 프로세스를 자동화하고 오케스트레이션 할 수 있도록 서비스 제공. 엔터프라이즈 환경에서 앱, 데이터 그리고 시스템의 통합을 지원

Azure Event Grid : 배포와 subscription 형태의 이벤트 소비를 위한 관리형 엔진 기반의 이벤트 라우팅 서비스

2. Understand Core Azure Services

Azure Storage Account (IaaS)

Block Blobs : Scalable object storage for VM, documents, videos, pictures, and unstructured text or binary data. Choose from Hot, Cool, or Archive tiers.

Azure Data Lake Storage : Combines the power of a Hadoop compatible file system with integrated hierarchical namespace with the massive scale and economy of Azure Blob Storage to help speed your transition from proof of concept to production.

Managed Disks : Persistent, secured disks that support simple and scalable virtual machine deployment. Designed for 99.999% availability. Choose Premium (SSD) Disks for low latency and high throughput.

Files : Fully managed file shares in the cloud, accessible via standard Server Message Block (SMB) protocol. Enables sharing files between applications using Windows APIs or REST API. Port no. : 445/TCP

Tables : NoSQL storage for unstructured and semi-structured data—ideal for web applications, address books, and other user data.

Queues : provide a reliable messaging solution for your apps, and are generally used to store messages to be processed asynchronously. Queue messages can be up to 64 KB in size and can contain millions of messages

Page Blobs : Page Blobs are optimized for random read and write options. Page Blobs are ideal for scenarios that require the ability to overwrite a random small segment at a known address, like storing index-based and sparse data structures. Page blobs can be accessed through REST protocol or attached to a VM to support disk traffic as Unmanaged Disks.

2. Understand Core Azure Services

Azure Storage Service : PaaS 서비스에 속함

Blob storage, File Storage, Table storage, Queue storage

Azure Data Box Family

Offline Data Transfer, Online Data Transfer 서비스가 있다. Offline Data box를 사용하는 이유는 회사마다 네트워크 대역폭에 제한을 걸어놓은 경우가 있어 속도가 느린 경우 이런 Azure Data Box를 사용한다.



Data Box



Data Box Disk



Data Box Heavy

2. Understand Core Azure Services

Recovery service vault

a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for virtual machines (VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services.

Azure File Sync

centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share. You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS. You can have as many caches as you need across the world.

2. Understand Core Azure Services

Azure Database Service : MS가 제공하는 RDBMS외에도 일반적으로 사용되는 DB도 지원한다.

Azure Cosmos DB, Azure SQL Database, Azure Database Migration

MS가 지원하는 RDBMS외에 외부 RDBMS를 사용한다면 High availability, 이중화는 고객이 알아서 해야 하지만 MS에서 기본적으로 자체 제공하는 RDBMS에는 자체적으로 High availability, 이중화를 제공하며 비용에 다 들어가 있다.

Azure Marketplace

고객들이 MS 파트너, ISVs(Independent Software Vendors) 그리고 스타트업의 솔루션 및 서비스를 Azure 상에서 사용할 수 있게 제공함.

2. Understand Core Azure Services

Internet of Things (IoT)

Microsoft IoT Central : 보다 손쉬운 IoT 서비스 구축을 위한 SaaS 형태의 관리형 서비스.
(디바이스 연결, 모니터 그리고 관리 및 확장 지원)

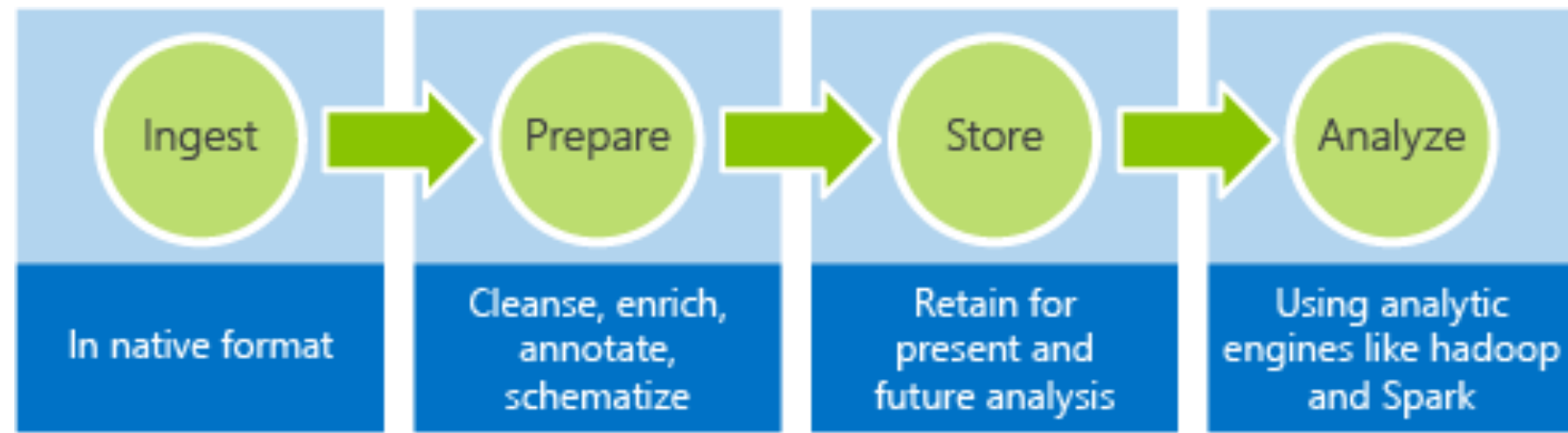
Azure IoT Hub : 클라우드 기반의 IoT 관리 플랫폼 서비스 (중앙 메시지 허브, 양방향 통신 및 관리)

Big Data & Analytics

Azure SQL Data Warehouse : 클라우드 기반으로 수십 페타의 데이터를 MPP 기반으로 빠르게 처리할 수 있는 서비스. High availability

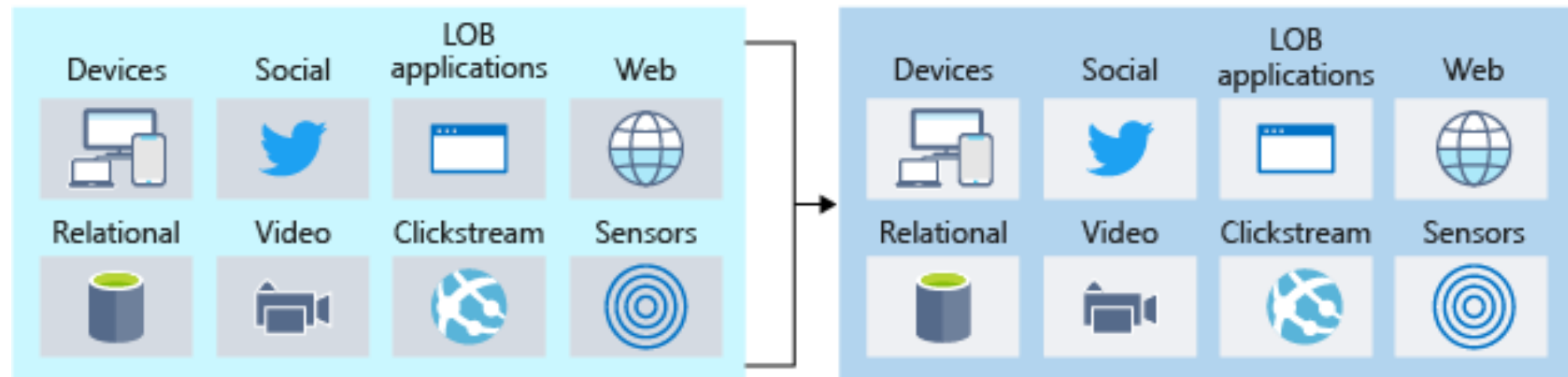
Azure HDInsight : 오픈소스 기반의 Hadoop을 관리되는 형태의 서비스로 제공. 쉽고 빠르게 비용 효율적으로 데이터 처리가 가능함

Azure Data Lake Analytics : 온디맨드 분석을 지원하는 서비스. 하드웨어 배포하는 대신 쿼리 기반으로 컴퓨팅을 할당하여 인사이트를 찾아낼 수 있는 서비스



- Batch queries
- Interactive queries
- Real-time analytics
- Machine Learning
- Data Warehouse

 Azure Data Lake Store



2. Understand Core Azure Services

Artificial Intelligence

클라우드 컴퓨팅의 맥락에서 인공지능(AI)은 기존 데이터를 사용하여 미래의 행동, 결과 및 추세를 예측하는 Machine running을 비롯한 광범위한 애플리케이션을 기반으로 함

Azure Machine Learning service : SDK 기반으로 손쉽게 코드 작성

Azure Machine Learning studio : GUI 기반으로 손쉽게 Machine running 을 만들고 테스트 배포할 수 있는 서비스 제공

Cognitive Services

A comprehensive family of AI services and cognitive APIs to help you build intelligent apps.

Cognitive Services bring AI within reach of every developer—without requiring machine-learning expertise.

2. Understand Core Azure Services

DevOps

DevOps를 사용하면 응용 프로그램에 대한 지속적인 통합, 제공 및 배포를 제공하는 빌드 및 릴리스 파이프라인 생성 지원 만들 수 있다.

Azure DevOps services : CI/CD for any platform, Agile planning tools, Unlimited free private repos, Manual and exploratory testing, Universal package repository

Azure DevTest Labs : enables developers on teams to efficiently self-manage virtual machines (VMs) and PaaS resources without waiting for approvals. Creates labs consisting of pre-configured bases or Azure Resource Manager templates. These have all the necessary tools and software that you can use to create environments. You can create environments in a few minutes, as opposed to hours or days.

2. Understand Core Azure Services

Azure 관리도구

- Azure Portal : Web portal (GUI)
- Azure PowerShell : Client-based shell based on Windows (.NET), Linux, or MacOS (.Net Core).
A module that you can install for Windows PowerShell or PowerShell Core
- Azure CLI : CLI for Windows, Linux and MacOS, Bash on Windows Subsystem for Linux(WSL)
WSL은 윈도우에서 리눅스 Bash 를 실행할 수 있게 해준다.
- Azure Cloud Shell : Web-based environment for PowerShell & Bash CLI. Windows, Linux and MacOS

Azure PowerShell은 기존 윈도우 PowerShell의 호환성을 위해 모듈로 제공되고 Azure CLI는 클라우드 상에서 돌아가는 다양한 OS를 지원하기 위해 제공된다.
- Azure mobile app : monitoring and managing your resources from your mobile device

2. Understand Core Azure Services

Azure Advisor

배포된 Azure 리소스를 분석하고 availability, security, performance 및 cost를 개선하는 방법과 정보를 제공. Azure AD 나 네트워크 관련 설정 제안은 하지 않음.

Azure Advisor 활용 예시 :

사전 예방적이고 실행 가능하며 Best Practice 기반의 개인화된 권장 사항 제공
리소스의 성능, 보안 및 가용성을 향상

Azure 비용을 절감할 수 있는 기회 제공

사용자가 놓치고 있는 권장 사항을 알려줌

2. Understand Core Azure Services

Azure Services - Compute

Service name	Service function
Azure Virtual Machines	Windows or Linux virtual machines (VMs) hosted in Azure
Azure Virtual Machine Scale Sets	Scaling for Windows or Linux VMs hosted in Azure
Azure Kubernetes Service	Enables management of a cluster of VMs that run containerized services
Azure Service Fabric	Distributed systems platform. Runs in Azure or on-premises
Azure Batch	Managed service for parallel and high-performance computing applications
Azure Container Instances	Run containerized apps on Azure without provisioning servers or VMs
Azure Functions	An event-driven, serverless compute service

2. Understand Core Azure Services

Azure Services - Networking

Service name	Service function
Azure Virtual Network	Connects VMs to incoming Virtual Private Network (VPN) connections
Azure Load Balancer	Balances inbound and outbound connections to applications or service endpoints
Azure Application Gateway	Optimizes app server farm delivery while increasing application security
Azure VPN Gateway	Accesses Azure Virtual Networks through high-performance VPN gateways
Azure DNS	Provides ultra-fast DNS responses and ultra-high domain availability
Azure Content Delivery Network	Delivers high-bandwidth content to customers globally
Azure DDoS Protection	Protects Azure-hosted applications from distributed denial of service (DDOS) attacks
Azure Traffic Manager	Distributes network traffic across Azure regions worldwide
Azure ExpressRoute	Connects to Azure over high-bandwidth dedicated secure connections
Azure Network Watcher	Monitors and diagnoses network issues using scenario-based analysis
Azure Firewall	Implements high-security, high-availability firewall with unlimited scalability
Azure Virtual WAN	Creates a unified wide area network (WAN), connecting local and remote sites

2. Understand Core Azure Services

Azure Services - Storage

Service name	Service function
Azure Blob storage	Storage service for very large objects, such as video files or bitmaps, VM
Azure File storage	File shares that you can access and manage like a file server. Port : 445
Azure Queue storage	A data store for queuing and reliably delivering messages between applications
Azure Table storage	A NoSQL store that hosts unstructured data independent of any schema

2. Understand Core Azure Services

Azure Services

These services all share several common characteristics:

Durable and highly available with redundancy and replication.

Secure through automatic encryption and role-based access control.

Scalable with virtually unlimited storage.

Managed handling maintenance and any critical problems for you.

Accessible from anywhere in the world over HTTP or HTTPS.

2. Understand Core Azure Services

Azure Services - Databases

Service name	Service function
Azure Cosmos DB	Globally distributed database that supports NoSQL options
Azure SQL Database	Fully managed relational database with auto-scale, integral intelligence, and robust security
Azure Database for MySQL	Fully managed and scalable MySQL relational database with high availability and security
Azure Database for PostgreSQL	Fully managed and scalable PostgreSQL relational database with high availability and security
SQL Server on VMs	Host enterprise SQL Server apps in the cloud
Azure SQL Data Warehouse	Fully managed data warehouse with integral security at every level of scale at no extra cost
Azure Database Migration Service	Migrates your databases to the cloud with no application code changes
Azure Cache for Redis	Caches frequently used and static data to reduce data and application latency
Azure Database for MariaDB	Fully managed and scalable MariaDB relational database with high availability and security

2. Understand Core Azure Services

Azure Services - Web

Service Name	Description
Azure App Service	Quickly create powerful cloud web-based apps (PaaS) - Runtime stack : Java, ASP.NET, Ruby, Python
Azure Notification Hubs	Send push notifications to any platform from any back end.
Azure API Management	Publish APIs to developers, partners, and employees securely and at scale.
Azure Cognitive Search	Fully managed search as a service.
Web Apps feature of Azure App Service	Create and deploy mission-critical web apps at scale.
Azure SignalR Service	Add real-time web functionalities easily.
Azure Application Insights	Detects and diagnoses anomalies in web apps

2. Understand Core Azure Services

Azure Services - Internet of Things

Service Name	Description
IoT Central	Fully-managed global IoT software as a service (SaaS) solution that makes it easy to connect, monitor, and manage your IoT assets at scale
IoT Hub	Messaging hub that provides secure communications and monitoring between millions of IoT devices
IoT Edge	Push your data analysis models directly onto your IoT devices, allowing them to react quickly to state changes without needing to consult cloud-based AI models.

2. Understand Core Azure Services

Azure Services - Big Data

Service Name	Description
Azure SQL Data Warehouse	Run analytics at a massive scale using a cloud-based Enterprise Data Warehouse (EDW) that leverages massive parallel processing (MPP) to run complex queries quickly across petabytes of data
Azure HDInsight	Process massive amounts of data with managed clusters of Hadoop clusters in the cloud
Azure Databricks	Collaborative Apache Spark-based analytics service that can be integrated with other Big Data services in Azure. A big data analysis service for machine learning

2. Understand Core Azure Services

Azure Services - Artificial Intelligence

Service Name	Description
Azure Machine Learning Service	Cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models. It can auto-generate a model and auto-tune it for you. It will let you start training on your local machine, and then scale out to the cloud
Azure Machine Learning Studio	Collaborative, drag-and-drop visual workspace where you can build, test, and deploy machine learning solutions using pre-built machine learning algorithms and data-handling modules
Azure AI Bot	Provide a digital online assistant that provides speech support

2. Understand Core Azure Services

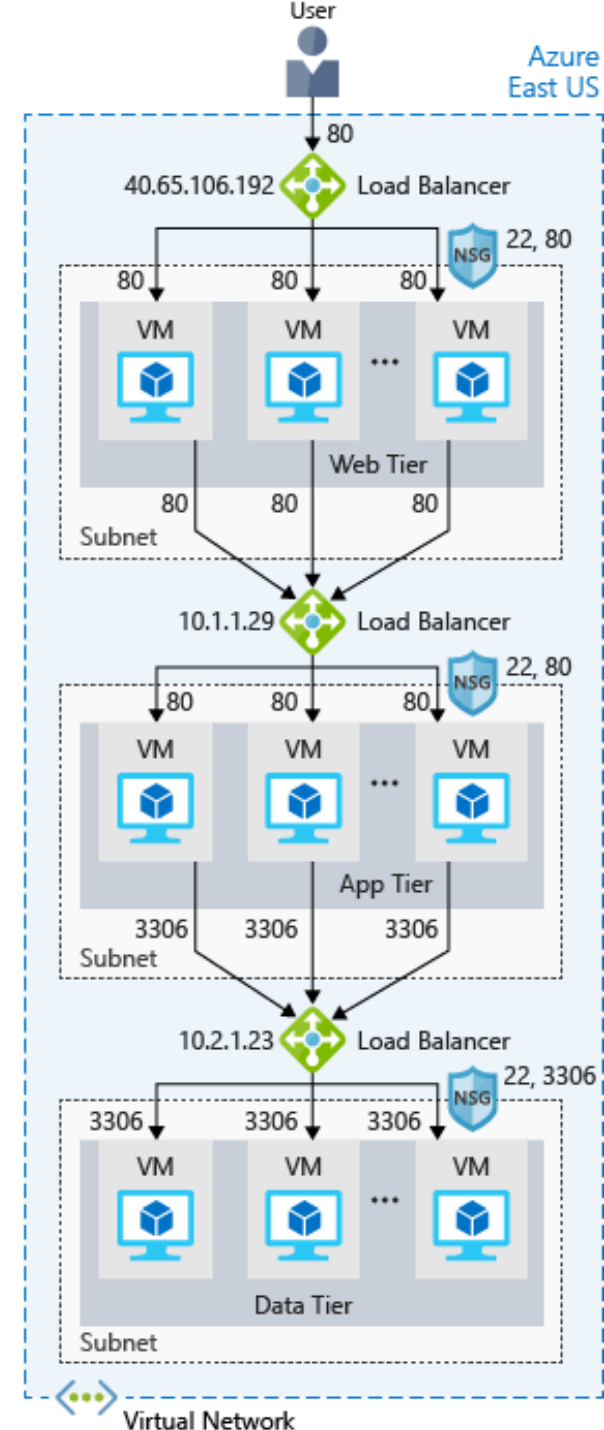
Azure Load Balancer

evenly distributing load (incoming network traffic) across a group of backend resources or servers. L

It's the single point of contact for clients. Load Balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances.

하나의 서버가 내려가면 나머지 살아있는 다른 서버로 넘겨준다

Transport level (TCP) 에서 작동한다.



2. Understand Core Azure Services

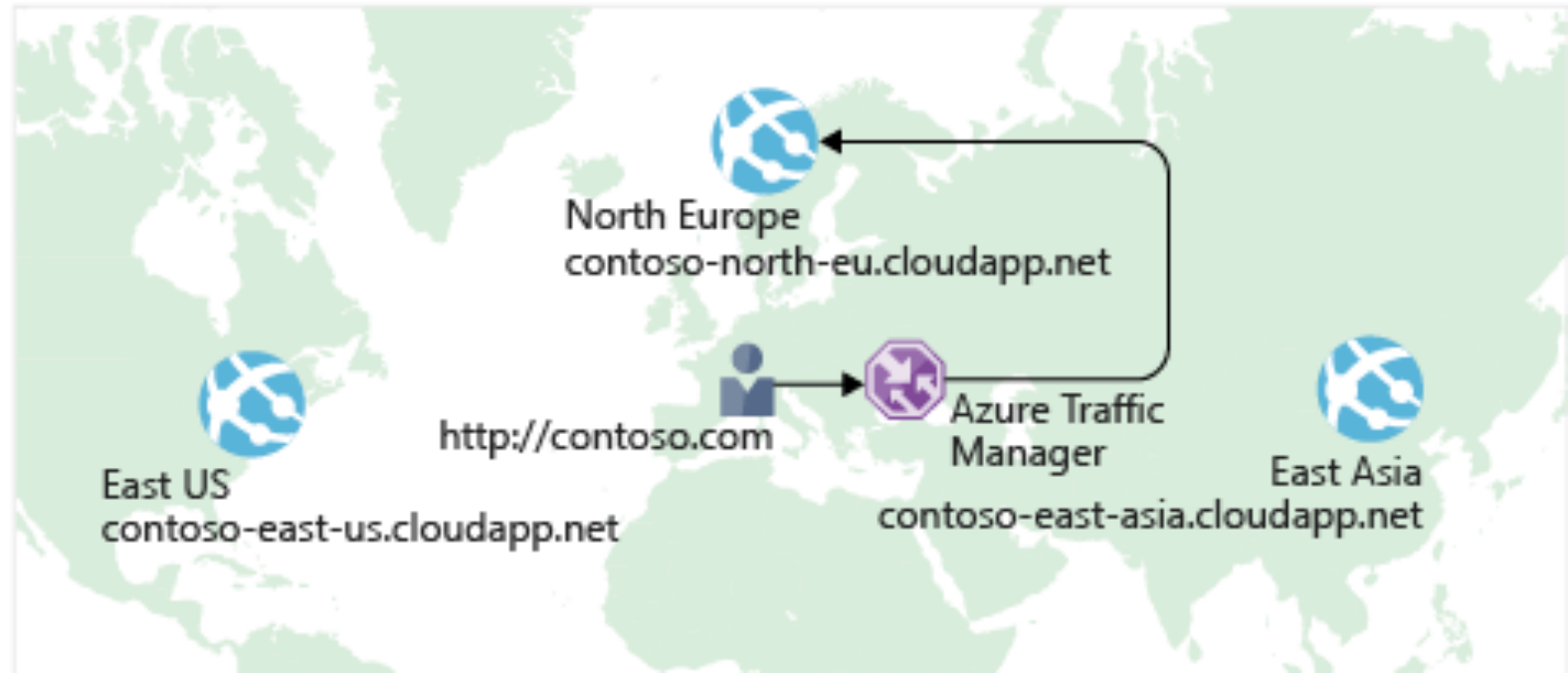
Azure Load Balancer (Continue..)

- Load balance internal and external traffic to Azure virtual machines.
- Increase availability by distributing resources within and across zones.
- Configure outbound connectivity for Azure virtual machines.
- Use health probes to monitor load-balanced resources.
- Employ port forwarding to access virtual machines in a virtual network by public IP address and port.
- Enable support for load-balancing of IPv6.
- Standard Load Balancer provides multi-dimensional metrics through Azure Monitor. These metrics can be filtered, grouped, and broken out for a given dimension. They provide current and historic insights into performance and health of your service. Resource Health is also supported. Review Standard Load Balancer Diagnostics for more details.
- Load balance services on multiple ports, multiple IP addresses, or both.
- Move internal and external load balancer resources across Azure regions.
- Load balance TCP and UDP flow on all ports simultaneously using HA ports.

2. Understand Core Azure Services

Traffic Manager

여러 Region에 인스턴스가 배치된 경우 DNS 서버를 사용하여 유저와 가장 가까운 globally distributed endpoint 로 트래픽을 보내준다. Load Balancer와 비슷하지만 Traffic Manager는 DNS 레벨에서 작동한다.



2. Understand Core Azure Services

Azure DNS

- You need to create a name server (NS) record for the zone.
- The **A Record points your hostname to an IP address.** The record A specifies IP address (IPv4) for given host. This is one of the most frequently used records in the DNS Zones.
- **PTR records are used for the Reverse DNS (Domain Name System) lookup.** Using the IP address you can get the associated domain/hostname. An A record should exist for every PTR record. The usage of a reverse DNS setup for a mail server is a good solution.
- The SOA means Start Of Authority. The **SOA record defines the beginning of the authority DNS zone and specifies the global parameters for the zone.** The SOA record has the following structure: "Serial number", "Primary name server (NS)", "DNS admin e-mail", "Refresh Rate", "Retry Rate", "Expire time" and "Default TTL".
- The **NS records identify the name servers, responsible for your DNS zone.** In order to have a valid DNS configuration, the NS records configured in the DNS zone must be exactly the same as these configured as name servers at your domain name provider.
- The root **TXT record for verification**
- A **CNAME record for the www name** that points to the A record

Module 3

Understand Security, Privacy, Compliance, and Trust

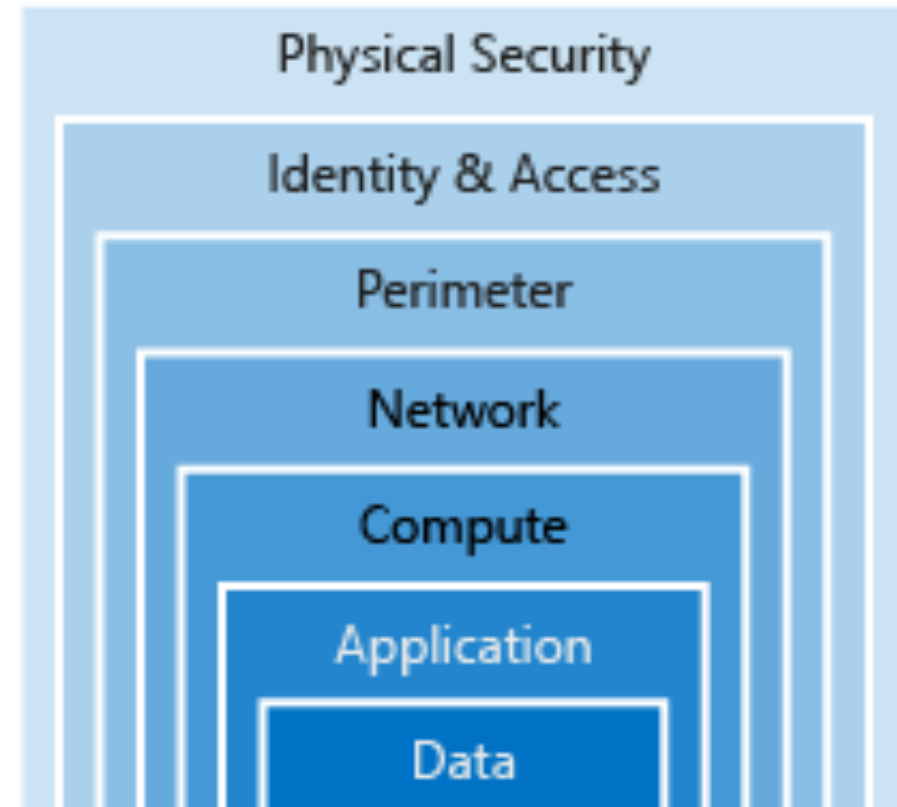
3. Understand Security, Privacy, Compliance, and Trust

Defense in Depth

컴퓨터 시스템 보안에 대한 단계적 접근 방식

여러 수준의 보호를 제공

한 레이어에 대한 공격은 후속 레이어에서 격리



3. Understand Security, Privacy, Compliance, and Trust

Azure Virtual Network (VNet)

Fundamental building block for a private network in Azure. (Network Layer level)

Enables to securely communicate with each other resource, the internet, and on-premises networks.

VNet is scoped to a single region/location; however, multiple virtual networks from different regions can be connected together using Virtual Network Peering

VNet is scoped to a subscription. Can implement multiple virtual networks within each Azure subscription and Azure region.

하나의 VNet에 여러 VM을 넣고 싶으면 그 VM들은 동일한 region에 위치해야한다.

3. Understand Security, Privacy, Compliance, and Trust

Azure Security Center

- Provide security recommendations based on configurations, resources, and networks.
- Monitor security settings across on-premises and cloud workloads, and automatically apply required security.
- Continuously monitor all your services, and perform automatic security assessments to identify potential vulnerabilities
- Use machine learning to detect and block malware. You can also define a list of allowed applications
- Analyze and identify potential inbound attacks, and help to investigate threats and any post-breach activity
- Provide just-in-time access control for ports, reducing your attack surface by ensuring the network only allows traffic

Free : limited to assessments and recommendations of Azure resources only

Standard : provide a full suite of security-related services including continuous monitoring, threat detection, just-in-time access control for ports., and more

3. Understand Security, Privacy, Compliance, and Trust

Azure Firewall

Stateful firewall as a service : filtering for both inbound and outbound traffic, hybrid connections through Azure VPN and ExpressRoute gateways

High availability and cloud scale : Azure Firewall automatically scales with your usage during peak load or as your business grows

Network- and application-level connectivity policies : Write policies that span fully-qualified domain name filtering for outbound HTTP(s) traffic and network filtering controls, using IP address, port and protocol

Intelligent near real-time security : alert and deny traffic from/to known malicious IP addresses and domains. The IP addresses and domains are sourced from the Microsoft Threat Intelligence feed.

Communicate with Internet resources using SNAT and DNAT : Source network address translation (SNAT), Destination Network Address Translation (DNAT).

Central logging and analytics : Use fully-integrated, built-in monitoring and reporting right in one place with Azure Monitor.

3. Understand Security, Privacy, Compliance, and Trust

Azure Application Gateway

An HTTP/HTTPS web traffic load balancer with URL-based routing, SSL, termination, session persistence, and Web Application Firewall (WAF) that provides protection from common, known vulnerabilities in websites. It is designed to protect HTTP/S traffic.

Application layer 에서 작동.

Azure Load Balancer

The single point of contact of clients. Distributes inbound flows to backend pool instances. These flows are according to configured load balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set. Employ port forwarding.

Transfer later 에서 작동.

3. Understand Security, Privacy, Compliance, and Trust

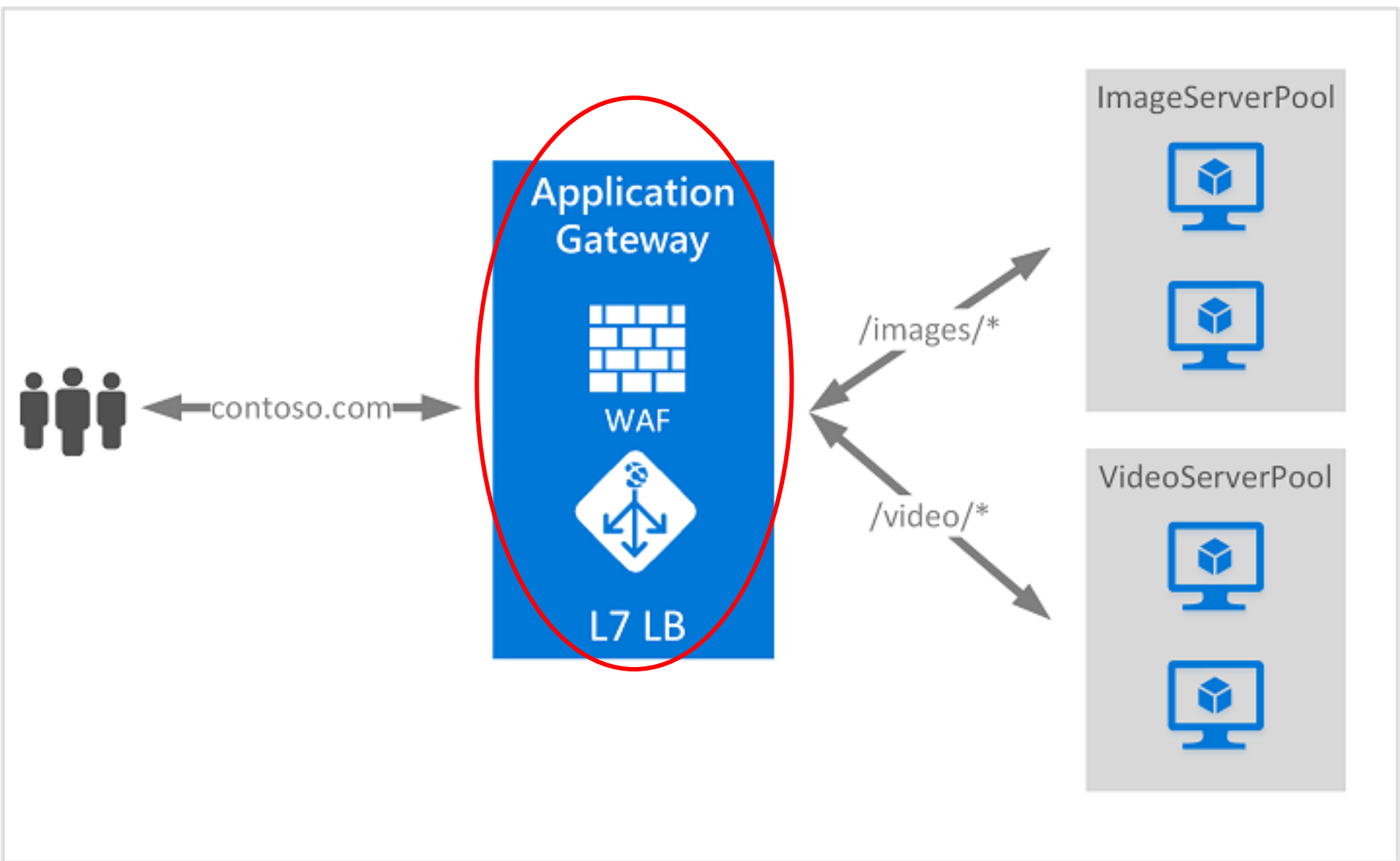
Network virtual appliances (NVAs)

are ideal options for non-HTTP services or advanced configurations, and are similar to hardware firewall appliances.

3. Understand Security, Privacy, Compliance, and Trust

Network Security Groups (NSGs)

- To simplify management of security rules, it's recommended that you associate a network security group to individual subnets, rather than individual network interfaces within the subnet, whenever possible.
- a critical piece to restrict unnecessary communication.
- Network Security Groups allow you to filter network traffic (inbound, outbound) to and from Azure resources in an Azure virtual network.
- An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol. They provide a list of allowed and denied communication to and from network interfaces and subnets, and are fully customizable.
- You can completely remove public internet access to your services by restricting access to service endpoints. With service endpoints, Azure service access can be limited to your virtual network.
- Azure Firewall을 한번 거치고 난 후 한번 더 거치는 기능을 제공. Application Security Groups 기능을 활용하여 서버 서비스 별로 Grouping하여 IP가 아닌 그룹 단위로 방화벽 룰이 적용되도록 함.

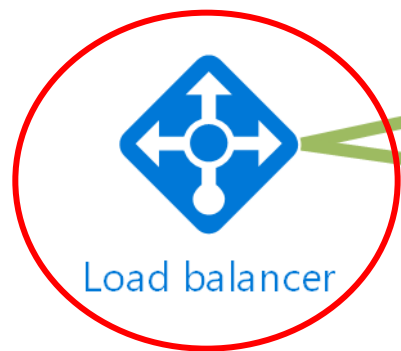




Azure Vnet
10.0.0.0/16

Public DMZ
10.0.0.64/27

Web tier
10.0.1.0/24



Availability
set



Availability
set



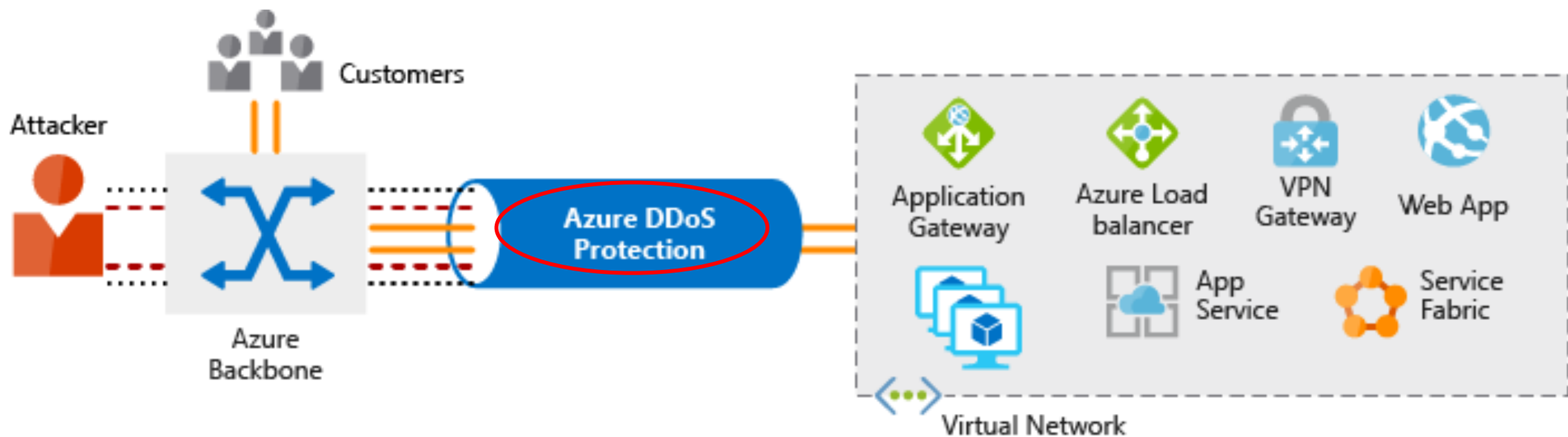
3. Understand Security, Privacy, Compliance, and Trust

Azure DDoS Protection

MS의 글로벌 네트워크의 scale과 elasticity를 leverage 하는 DDoS 공격 보호 기능. 사용자의 service availability에 영향을 미치기 전에 Azure network 에서 트래픽 모니터링을 함.

Basic : 기본적으로 제공하는 tier. 항상 네트워크 레벨에서 트래픽을 실시간으로 모니터링한다. Azure global network는 공격 트래픽을 여러 region에 걸쳐 분배하고 그 영향을 최소화한다.

Standard : Machine running 알고리즘을 사용하며 Volumetric attacks, Protocol attacks, Resource(application) layer attacks 에서의 공격을 최소화한다.



3. Understand Security, Privacy, Compliance, and Trust

Azure VPN Gateway

VNet-to-VNet 연결 가능. connect a virtual network to another virtual network with a VNet-to-VNet connection type (VNet2VNet).

여러 Region에 걸쳐 있는 VNet 간 연결 가능하게 해준다.

- IKEv2 : Windows, Linux, MacOS, Android, and iOS
- SSTP : Windows

3. Understand Security, Privacy, Compliance, and Trust

Azure VPN Gateway (Continue..)

A VPN gateway is used when creating a VPN connection to your on-premises network.

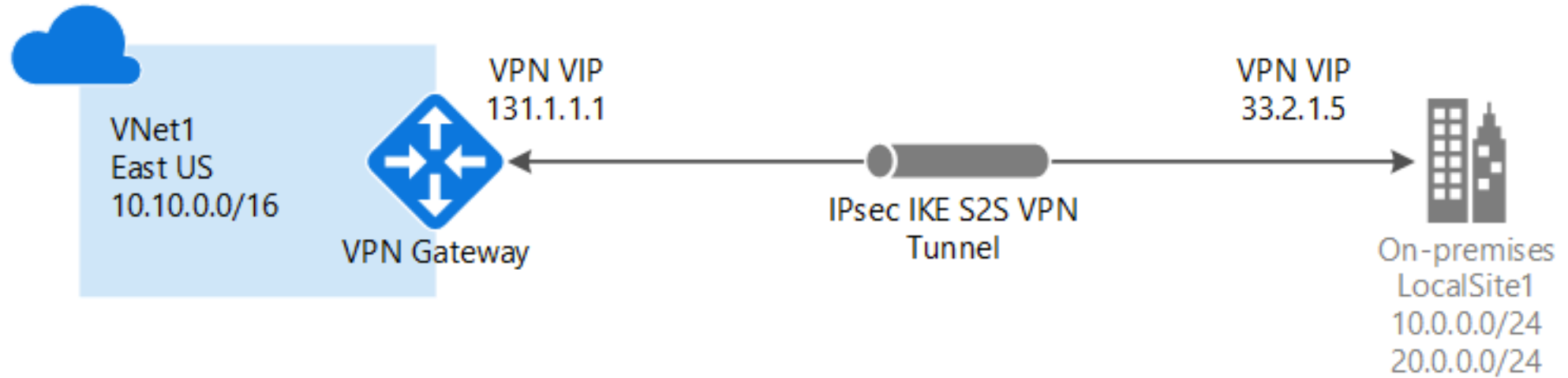
Route-based VPN devices use **any-to-any (wildcard) traffic** selectors, and let routing/forwarding tables direct traffic to different IPsec tunnels. It is typically built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface).

Policy-based VPN devices use the combinations of prefixes from both networks to define how traffic is encrypted/decrypted through IPsec tunnels. It is **typically built on firewall devices that perform packet filtering**. IPsec tunnel encryption and decryption are added to the packet filtering and processing engine.

Point-to-Site connections **do not require a VPN device** or a public-facing IP address.

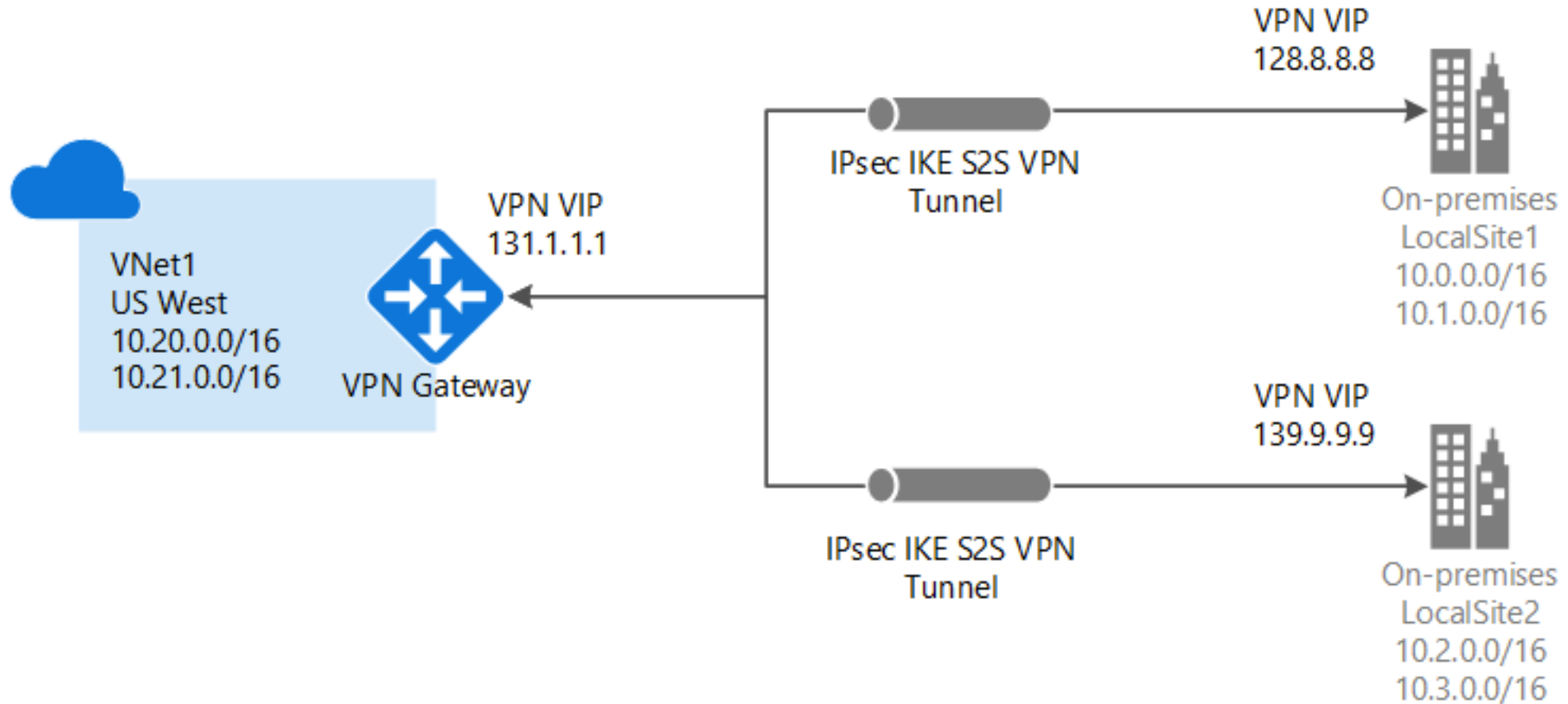
Site-to-Site and Multi-Site (IPsec/IKE VPN tunnel)

Site-to-Site

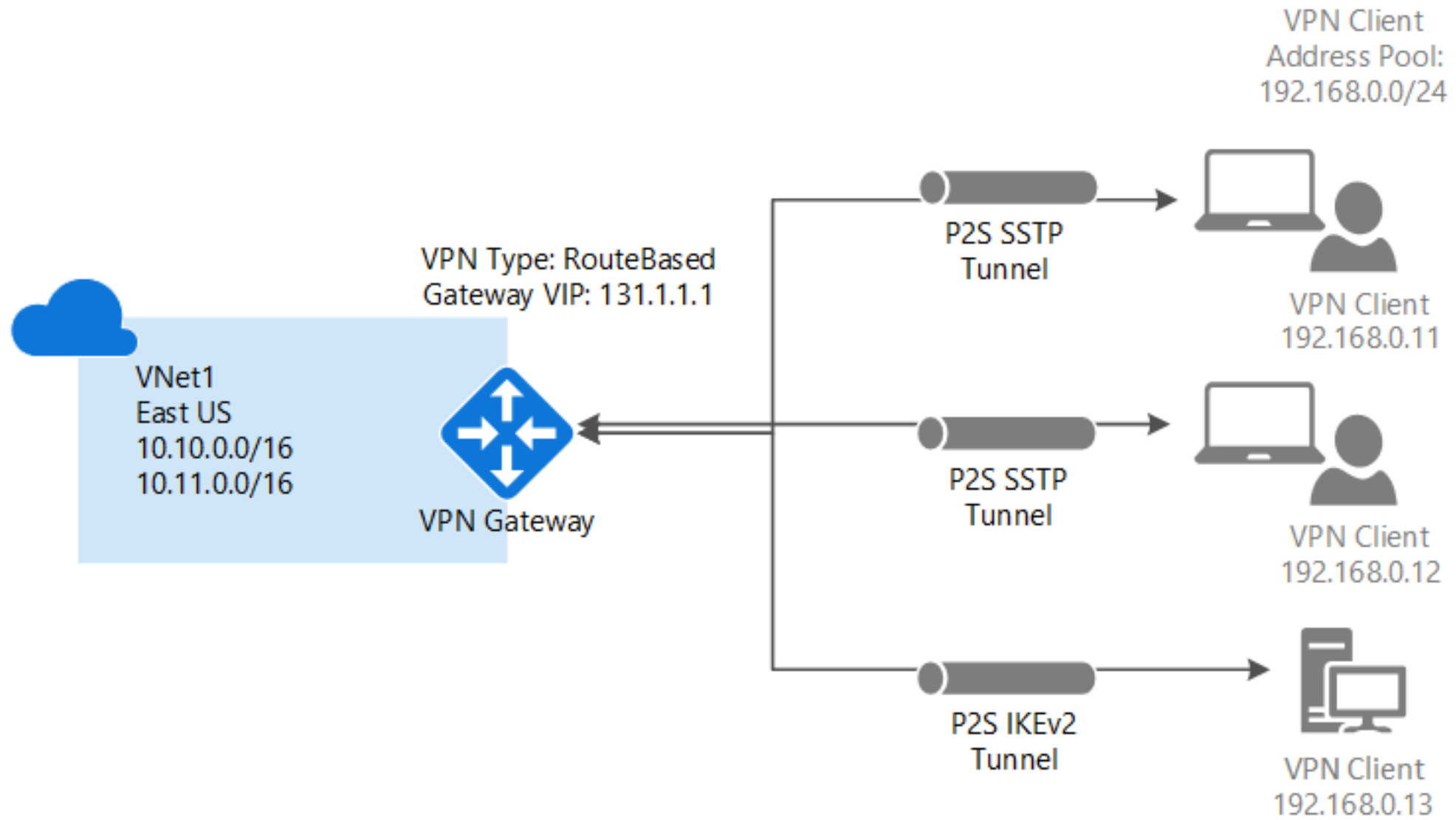


Site-to-Site and Multi-Site (IPsec/IKE VPN tunnel)

Multi-Site

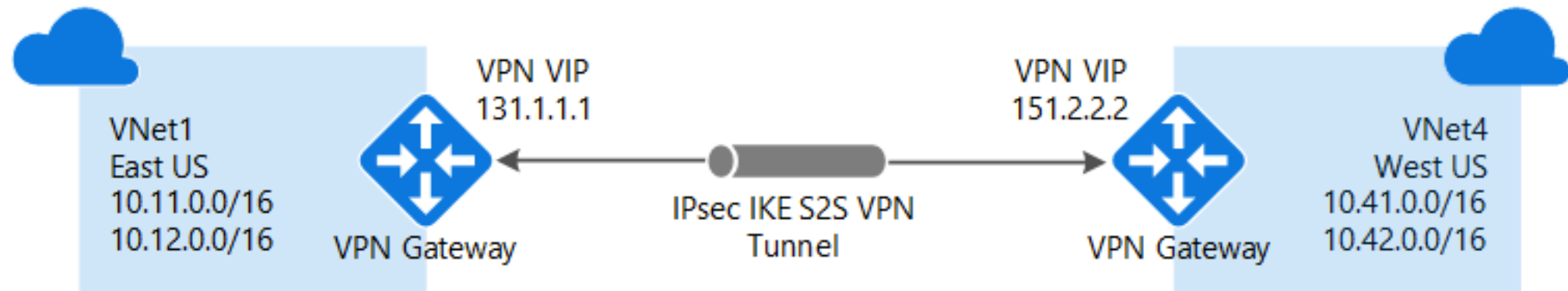


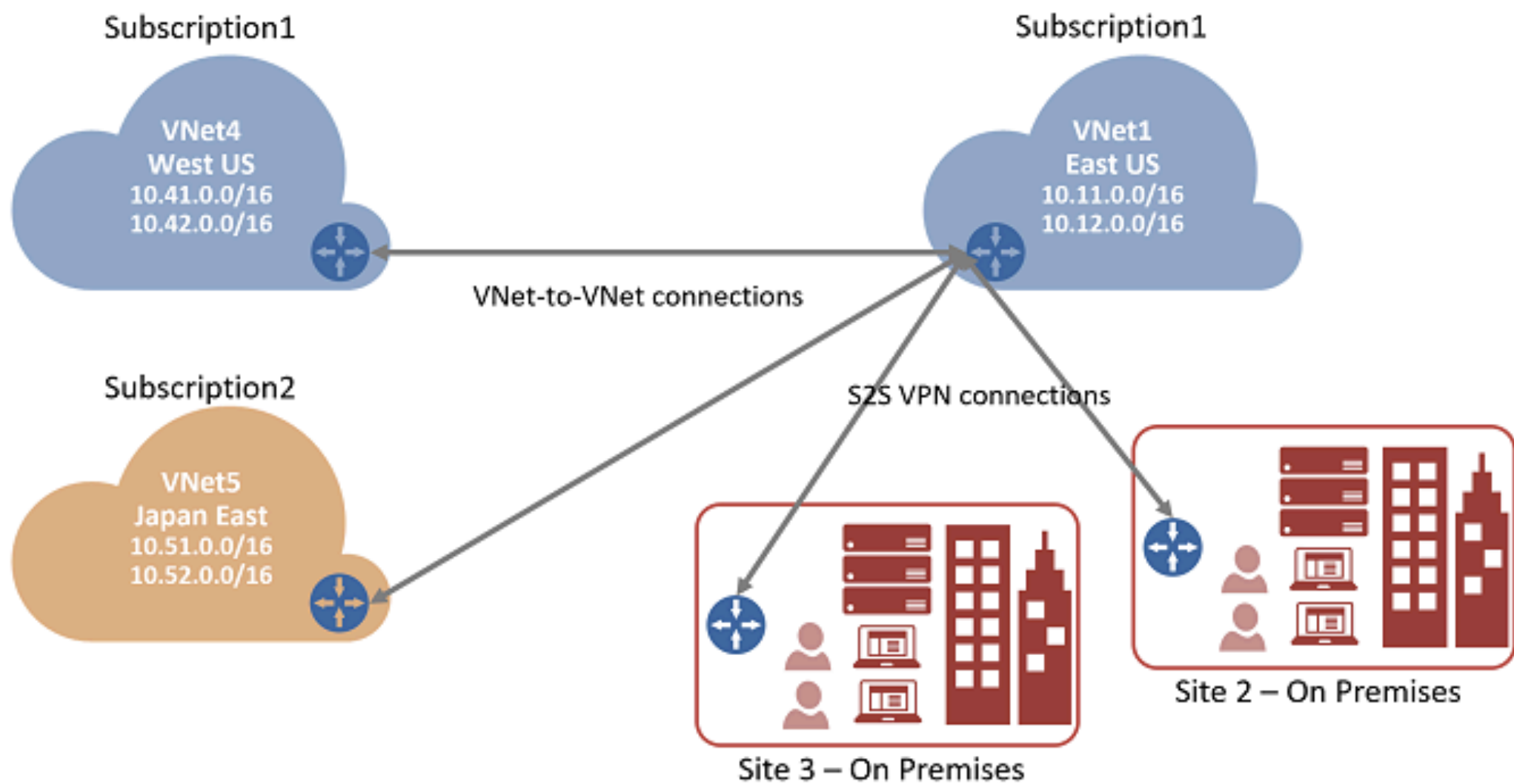
Point-to-Site VPN



VNet-to-VNet connections (IPsec/IKE VPN tunnel)

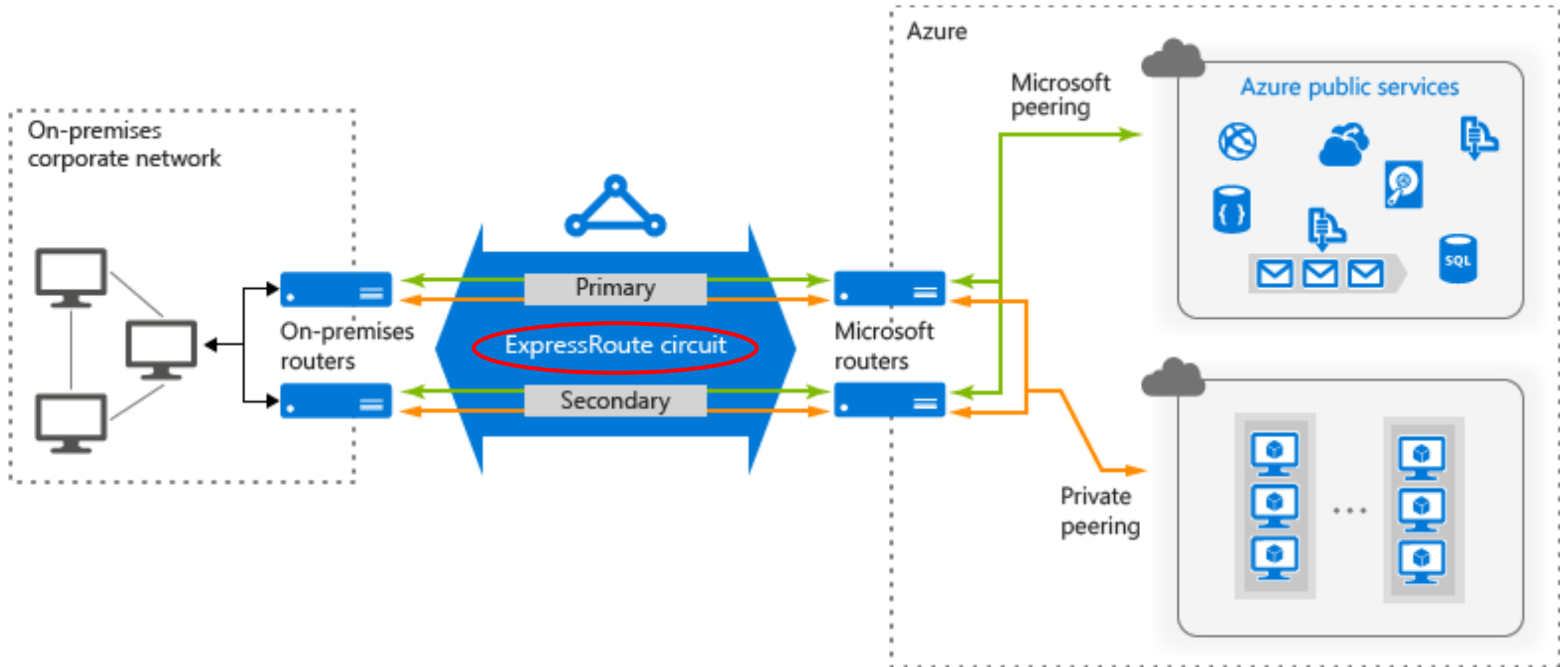
- in the same or different regions
- in the same or different subscriptions
- in the same or different deployment models



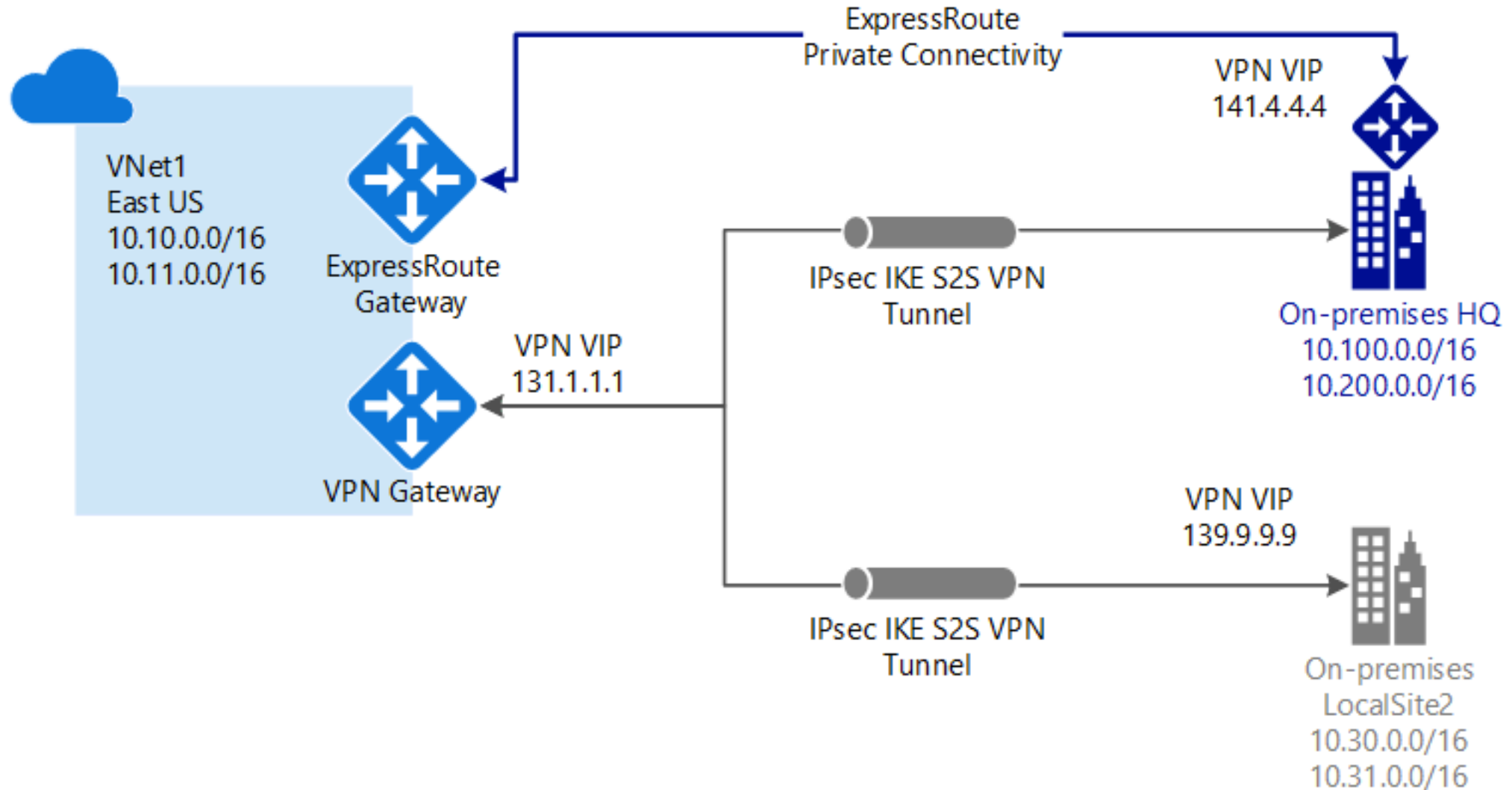


ExpressRoute (private connection)

On-premises network 와 Azure의 VNet (Azure Virtual Network)을 VPN을 통해 연결하여 Public internet과의 접촉없이 안전하게 연결 가능



Site-to-Site and ExpressRoute coexisting connections



3. Understand Security, Privacy, Compliance, and Trust

인증 및 권한 부여

Authentication

리소스에 대한 액세스를 원하는 사람 또는 서비스를 식별

합법적인 액세스 자격 증명을 요청

보안 ID 및 액세스 제어 원칙을 만들기 위한 기반을 마련

process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

Authorization

어떤 데이터에 접근 권한이 있는지 그 범위를 적용

security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features. Authorization is normally preceded by authentication for user identity verification. System administrators (SA) are typically assigned permission levels covering all system and user resources.

3. Understand Security, Privacy, Compliance, and Trust

Azure Active Directory

AD Identity Protection : enables organizations to configure automated responses to detected suspicious actions related to user identities.

Authentication : ID verification to access application, resources, self-service PW reset, MFA, smart lockout, custom banned PW list

Single-Sign-On (SSO) : reducing the effort needed to change or disable accounts

Application management : Manage cloud and on-premises apps using Azure AD Application Proxy, SSO, My apps portal, SaaS apps.

B2B identity services : guest users and external partners 관리, sign up, sign in, profile 컨트롤

Device Management : cloud or on-premises device 관리

3. Understand Security, Privacy, Compliance, and Trust

Encryption

Azure Storage Service Encryption - storage

Raw storage를 암호화해주며 아래 서비스들에 적용됨

Azure Managed Disks, Azure Blob storage, Azure Files, Azure Queue

Azure Disk Encryption - VM

Raw storage외에 OS가 담긴 VHD(Virtual hard disk)를 BitLocker(윈도우)나 dm-crypt(리눅스)를 이용하여 OS와 데이터 디스크를 위한 볼륨 암호화. Azure Key Vault와 통합되어 암호화 키를 저장함

Transparent data encryption (TDE) - DB

Azure SQL Database, Azure Data Warehouse 의 데이터베이스, 연관 백업, Transaction 로그파일을 암호화

3. Understand Security, Privacy, Compliance, and Trust

Azure Information Protection (AIP)

예를 들어 워드 문서나 전자 메일에 신용카드 번호 등의 개인정보가 담긴 경우 레이블을 수동으로 적용하여 분류하고 보호

Analyze data flows to gain insight into your business

Detect risky behaviors and take corrective measures

Track access to documents

Prevent data leakage or misuse of confidential information

- * Which labels are included that let administrators and users classify (and optionally, protect) documents and emails.
- * Title and tooltip for the Information Protection bar that users see in their Office applications.
- * The option to set a default label as a starting point for classifying documents and emails.
- * The option to enforce classification when users save documents and send emails.
- * The option to prompt users to provide a reason when they select a label that has a lower sensitivity level than the original.
- * The option to automatically label an email message, based on its attachments.
- * The option to control whether the Information Protection bar is displayed in Office applications.
- * The option to control whether the Do Not Forward button is displayed in Outlook.
- * The option to let users specify their own permissions for documents.
- * The option to provide a custom help link for users.

3. Understand Security, Privacy, Compliance, and Trust

Azure Advanced Threat Protection (Azure ATP)

is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

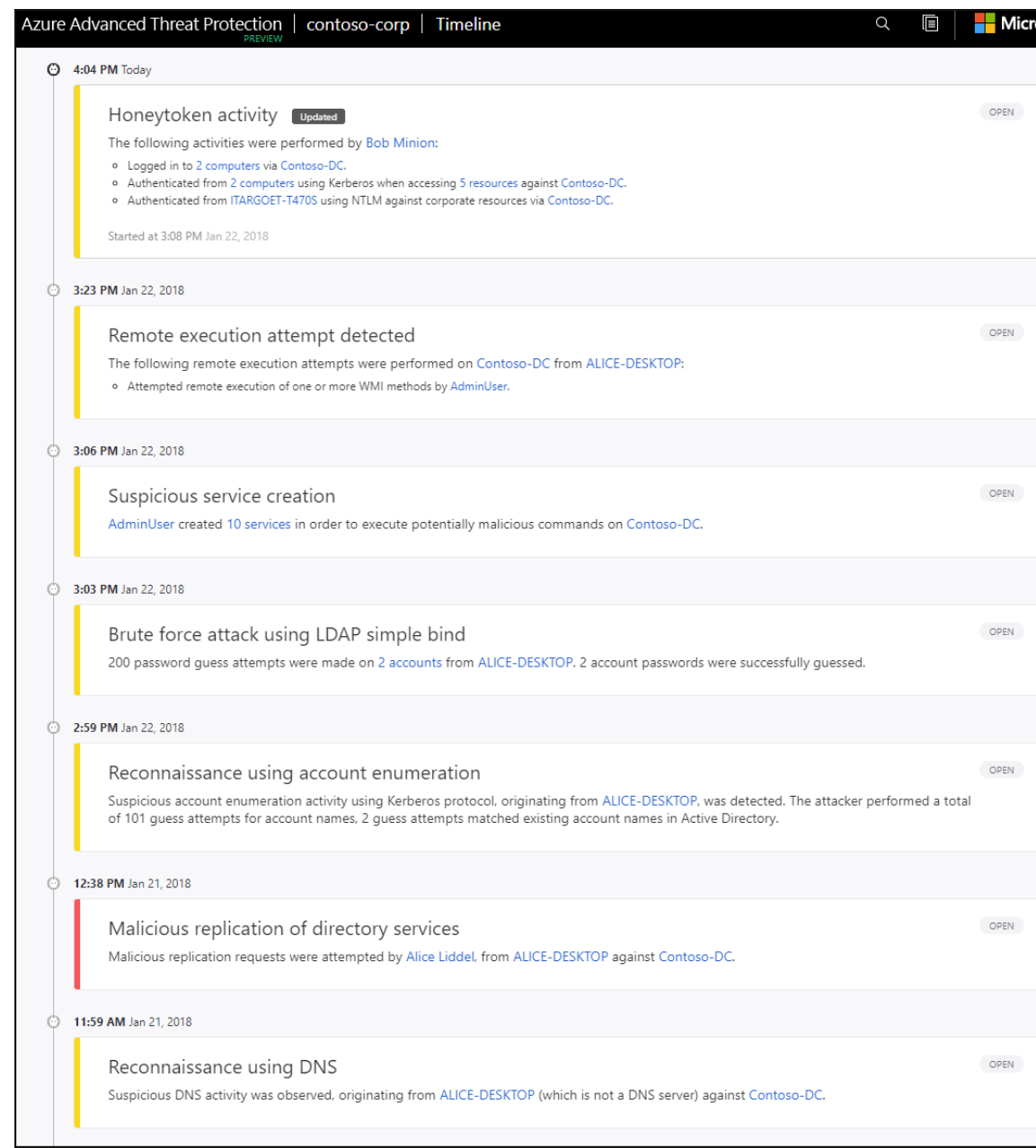
Installed directly on your domain controllers, the Azure ATP sensor accesses the event logs it requires directly from the domain controller. After the logs and network traffic are parsed by the sensor, Azure ATP sends only the parsed information to the Azure ATP cloud service

3. Understand Security, Privacy, Compliance, and Trust

Azure ATP portal : suspicious activity을
모니터링하고 대응하기 위한 전용 포털
<https://portal.atp.azure.com>

Azure ATP sensor : 도메인 컨트롤러에 직접
설치되어 domain controller traffic을 전용 서버나
포트미러링 없이 모니터링 가능하게 해줌

Cloud Service : Azure 인프라에서 직접 실행



3. Understand Security, Privacy, Compliance, and Trust

Azure Key Vault

Centralized application secrets, Securely stored secrets and keys, Monitor access and use, Simplified administration of application secrets, Integrate with other Azure service

응용 프로그램 보안을 중앙집중식 클라우드 위치에 저장하여 액세스 권한을 안전하게 제어함 (접근 등에 대한 로깅 및 관리)

Secret management, Key management, Certificate management, Store secrets backed by hardware security modules(HSM)을 지원하는 장비에 저장된 비밀번호 정보가져오기 지원

3. Understand Security, Privacy, Compliance, and Trust

규정 준수 약관 및 요구 사항

MS는 다른 클라우드 서비스 공급자보다 가장 포괄적인 compliance offerings(인증 및 증명 포함)을 제공

Global, US Gov, Industry, Region 별 등으로 세분화되어 있음

Microsoft Privacy Statement

MS가 제품, 서비스, 웹사이트, 앱, 서버, 기기에서 수집한 사용자 데이터를 처리하는 방법에 대해 개방적이고 정직하게 제공

You can obtain the details about how Microsoft uses personal data in the Microsoft Privacy Statement.

3. Understand Security, Privacy, Compliance, and Trust

Trust Center

<https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home>

- In-depth information about security, privacy, compliance offerings, policies, features, and practices
- Recommended resources in the form of a curated list of the most applicable and widely-used resources
- Information specific to key organizational roles, including business managers, tenant admins or data security teams, risk assessment and privacy officers, and legal compliance teams.
- Cross-company document search, which is coming soon and will enable existing cloud service customers
- Direct guidance and support for when you can't find what you're looking for.

3. Understand Security, Privacy, Compliance, and Trust

Service Trust Portal (STP)

<https://servicetrust.microsoft.com/>

- hosts the Compliance Manager service, and is the Microsoft public site for publishing audit reports and other compliance-related information
- STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored reports
- information about how Microsoft online services can help your organization maintain and track compliance with standards, laws, and regulations, such as: ISO, SOC, NIST, FedRAMP, GDPR

3. Understand Security, Privacy, Compliance, and Trust

Compliance Manager

<https://servicetrust.microsoft.com/ComplianceManager>

workflow-based risk assessment dashboard within the Trust Portal that enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft

- Enables you to assign, track, and record compliance and assessment-related activities, which can help your organization cross team barriers to achieve your organization's compliance goals.
- Provides a Compliance Score to help you track your progress and prioritize auditing controls that will help reduce your organization's exposure to risk.
- Provides a secure repository in which to upload and manage evidence and other artifacts related to compliance activities.
- Produces richly detailed reports in Microsoft Excel that document the compliance activities performed by Microsoft and your organization, which can be provided to auditors, regulators, and other compliance stakeholders.

3. Understand Security, Privacy, Compliance, and Trust

Monitoring and reporting in Azure

Azure Monitor

cloud 및 on-premise Metrics와 Logs 데이터를 활용하여 Insights, Visualize, Analyze, Response, Integrate 를 할 수 있다.

maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.

Azure Insights : monitor your live applications. automatically detect performance anomalies, and includes powerful analytics tools

Activity Log : Determine the what, who, and when for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. You can also understand the status of the operation and other relevant properties. The Activity Log does not include read (GET) operations or operations for resources that use the Classic/RDPE model.

Log Analytics : correlate events from multiple resources into a centralized repository. a web tool used to write and execute Azure Monitor log queries.

Azure Service Status

Azure service issues를 확인할 수 있도록 개인화된 뷰, 알림 및 문제 해결 업데이트 등의 정보를 제공

Azure Status : 전세계 여러 지역의 Region별로 제품 및 서비스 상태를 한눈에 볼 수 있다

Service Health : Provides up-to-date status information about the health of Azure services (subscription, region, resource)

Resource Health : 각종 상태 히스토리 로그 표시

3. Understand Security, Privacy, Compliance, and Trust

Monitoring and reporting in Azure

Event Hubs

a fully managed, real-time data ingestion service that's simple, trusted, and scalable. Stream millions of events per second from any source to build dynamic data pipelines and immediately respond to business challenges. Keep processing data during emergencies using the geo-disaster recovery and geo-replication features. **Integrate seamlessly with other Azure services to unlock valuable insights.** Allow existing Apache Kafka clients and applications to talk to Event Hubs without any code changes—**you get a managed Kafka experience without having to manage your own clusters.** Experience real-time data ingestion and microbatching on the same stream.

3. Understand Security, Privacy, Compliance, and Trust

Resource groups

Is a logical container for resources deployed on Azure

Its components can be anything like VM, Application Gateways and CosmosDB instances

All resources must be in a resource group and a resource can only be a member of a Single resource group

Many resources can be moved between resource groups with limitations and requirements to move

Resource groups can't be nested. Before any resource can be provisioned, you need a resource group for it to be placed in.

If you delete a resource group, all resources contained within are also deleted. It is useful in non-production environments

Resource groups are also a scope for applying RBAC permission.

Can be created by Azure portal, PowerShell, CLI, Templates, SDKs like .NET, Java



Resource groups are a scope of RBAC

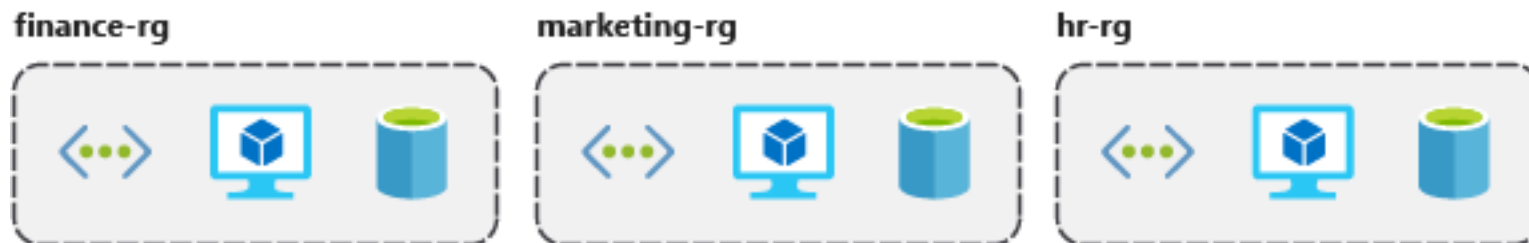
Organized by resource type (Vnets, VM, DB)



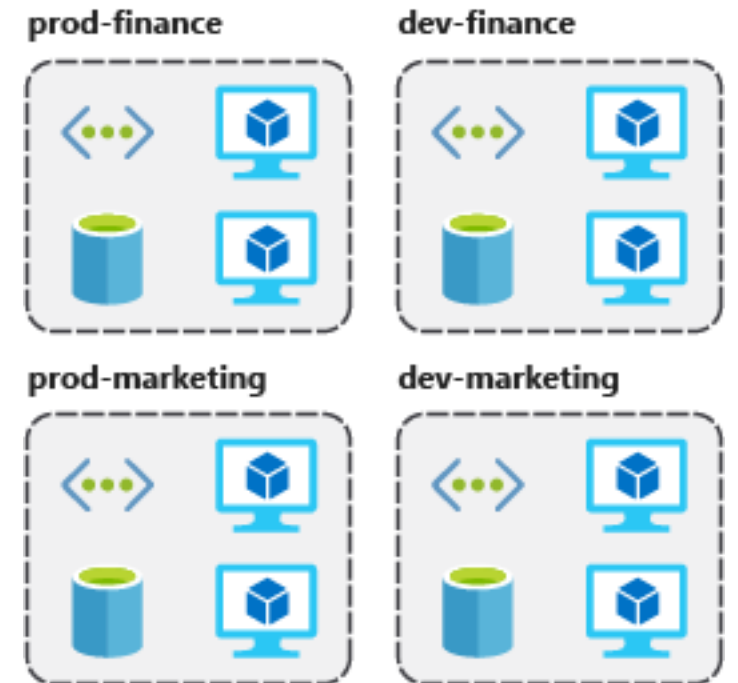
Organized by environment (prod, qa, dev)



Organized by department (marketing, finance, HR)



Combination of these strategies
Organized by environment and department



3. Understand Security, Privacy, Compliance, and Trust

Tag

관리를 위해 Azure 리소스에 Tag 메타 데이터를 설정함으로써 워크로드, 부서, life cycle, automation, 환경 별 비용 및 모니터링 등이 가능함

태그는 청구 및 관리 용도로 활용

리소스 그룹에 할당된 Tag는 inherit/propagate 되지 않음.

Tag를 지원하지 않는 리소스도 일부 있음

해당 Subscription의 워크로드에 대한 비용을 최적화, Azure Automation과 연계하여 schedule maintenance windows에 활용, 부서 간 internal chargeback 관련 cost center 연계하여 사용 가능

3. Understand Security, Privacy, Compliance, and Trust

Azure Policy

Azure 리소스에 대한 법규, 규칙 적용 및 제어를 위해 Policy를 사용하여 회사 표준 및 SLA를 준수 가능. Naming policy, 비용 절감을 위해 VM 사이즈 제한 가능

Policy를 준수하지 않는 Azure 리소스를 평가하고 식별. **Default allow and explicit deny system.**

Allowed Storage Account SKUs : 조건 및 규칙은 새 저장소 계정에 허용되는 크기를 정의. 정의된 크기 이외의 저장소 계정을 만드는 요청은 거부.

Allowed Resource Type : 조직에서 리소스를 배포할 수 있는 Azure 위치를 정의하여 지리적 규정 준수 요구 사항 만족. 정의된 위치 외부에 리소스를 배포하는 요청은 거부

Allowed Locations : 특정 region에만 리소스를 배치할지 규제 가능

Allowed Virtual Machine SKUs : 허용할 VM 종류

Not allowed resource types : 허용하지 않을 VM 종류

3. Understand Security, Privacy, Compliance, and Trust

Policy Initiatives

Initiatives work alongside policies in Azure Policy. An initiative definition is a set or group of policy definitions to help track your compliance state for a larger goal. Initiative definitions : 여러 정책 정의를 단일 단위로 그룹화하여 더 큰 수준 범위에서 규정 준수를 추적 가능.

Initiative assignments : Initiative definitions을 적용한 리스트

Role-based access control (RBAC)

Azure 리소스에 대한 fine-grained access management 제공

추가 비용 없이 모든 Azure subscription 자가 이용 가능

Allow one user to manage VMs in a subscription, and another user to manage virtual networks.

Allow a database administrator (DBA) group to manage SQL databases in a subscription.

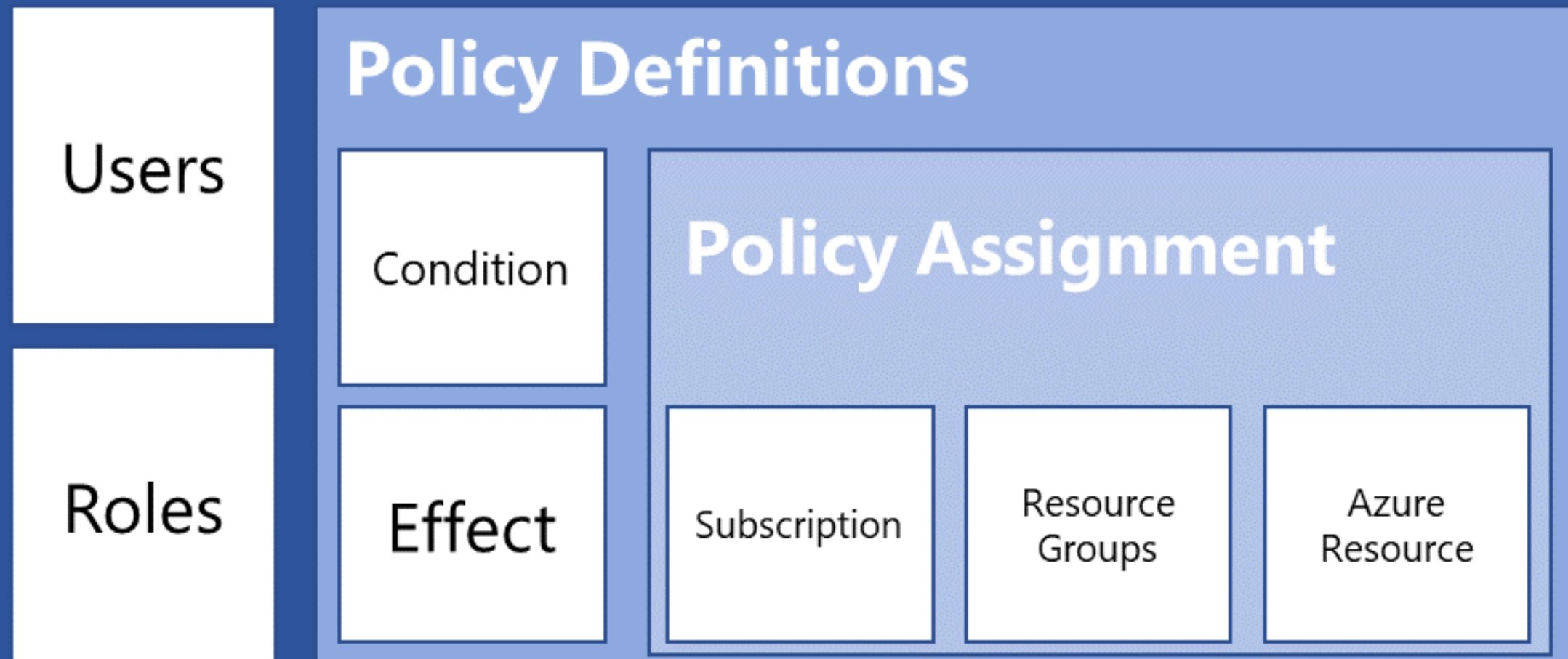
Allow an application to access all resources in a resource group.

Allow a user to manage all resources in a resource group, such as VMs, websites, and virtual subnets.

Access control (IAM) 메뉴를 통해 Permission 확인 가능

Allow model

Role Based Access Control (RBAC)



3. Understand Security, Privacy, Compliance, and Trust

Locks

실수로 삭제하거나 수정하지 않도록 Azure 리소스를 보호. Read-only, Delete 설정 및 추가 가능
Azure Portal 내의 subscription, resource group 또는 개별 resource 수준에서 잠금을 관리. (inheritable)

Azure Blueprints

재사용 가능한 정의를 만든 후 리소스 생성 및 정책을 한꺼번에 적용할 수 있게 함.

기본 제공 도구 및 아티팩트를 사용하여 배포를 감사하고 추적하고 규정 준수 유지.

Blueprint를 특정 Azure DevOps 빌드 artifacts 및 release pipeline 연결하여 엄격한 추적을 수행

JASON 방식으로 템플릿을 추출하고 재사용할 수 있다. 버전 관리, 추적 기능 제공.

ARM 컨트롤보다 좀 더 다양한 기능을 제공

Resource groups, policies, role assignment, Resource Manager template 으로 구성되어 있다.

Resource Manager templates 를 재사용할 수 있다.

Module 4

Understand Azure Pricing and Support

4. Understand Azure Pricing and Support

Azure 비용을 계획하고 관리하는 방법

Azure Support 지원 옵션 이해

Azure SLA 기능 이해 및 설명

Azure 제품 및 서비스 구매

Enterprise : Enterprise Agreement Azure 계약을 가진 고객. 보통 연간 계약 구조를 가짐

Web direct : 웹사이트를 통해서 바로 사용 및 계약하는 고객 Pay-as-you-go

Cloud solution providers (CSPs) : MS 파트너사로 고객이 Azure 상에서 솔루션 구현을 위해 고용하는 형태. 비용은 고객의 파트너사를 통해서 과금 및 지불되는 구조

지출 한도에 도달하면 리소스는 전부 제거되고 할당 취소된다. 하지만 스토리지 계정의 데이터는 읽기 전용으로 일정 기간 동안 액세스가 가능하다.

4. Understand Azure Pricing and Support

비용에 영향을 미치는 요인

Resource Type : 비용은 리소스에 따라 다르기 때문에 meter가 추적하는 사용량과 리소스와 연결된 meter수는 리소스 유형에 따라 다르다. (Compute Hours, IP Address Hours, Data Transfer In/Out, Standard Managed Disk/Operations, Standard IO-Disk, Standard IO-Block Blob Read/Write/Delete)

Services : Azure 사용 요율 및 청구 기간은 계약 방식에 따라 다를 수 있다

Location : Azure 인프라는 전세계적으로 분산되어 있어 사용 비용은 특정 Azure 제품, 서비스 및 리소스를 제공하는 위치에 따라 다를 수 있다. Region 중 유난히 저렴한 곳이 있으므로 굳이 지역적 특성이 필요 없다면 이런 지역적 이점을 활용할 수 있다.

기본적으로 usage에 기반하여 charge 되는데 예를 들어 de-allocate 된 VM은 computer hours, I/O reads/writes, 사설 IP 비용은 청구되지 않지만 디스크의 storage 는 비용이 발생한다. (사용자의 데이터가 디스크에 보관되어 있는 것을 디스크를 사용한다고 보기 때문)

4. Understand Azure Pricing and Support

요금 청구를 위한 Zones 개념

Azure ingress (inbound) network traffic은 무료

Egress (outbound) network traffic 과금은 Zone에 따라 다름 (Availability Zone과 다름. 과금에만 적용.)
들어올 때는 무료지만 나갈 때는 유료이다.

기본적으로 5GB/월 무료이며 GB 당 고정 요금이 적용된다.

Zone	Areas
Zone 1	United States, US Government, Europe, Canada, UK, France, Switzerland
Zone 2	East Asia, Southeast Asia, Japan, Australia, India, Korea
Zone 3	Brazil, South Africa, UAE
DE Zone 1	Germany

4. Understand Azure Pricing and Support

Azure Pricing calculator

<https://azure.microsoft.com/en-us/pricing/calculator/>

필요한 특정 요구 사항에 따라 구성하고 발생 가능한 비용을 예측

Azure services 와 속성 값을 넣으면 서비스 별 비용과 총 예상 비용이 산출된다.

Region, Tier, Billing Options, Support Options, Programs and Offers, Azure Dev/Test Pricing 등이 선택 가능한 구성요소

Products 탭을 눌러 견적서를 엑셀 파일로 추출 및 URL 공유할 수 있다

Azure TCO Calculator

<https://azure.microsoft.com/en-us/pricing/tco/calculator/>

On-premise 에서 Azure로 마이그레이션할 경우 발생할 Total Cost of Ownership (TCO) 확인 및 비용 절감 예측

이 보고서는 On-premise 인프라의 비용과 Azure 제품 및 서비스를 Cloud에서 인프라를 호스트하는데 드는 비용을 비교. ROI 정보를 제공한다.

4. Understand Azure Pricing and Support

Azure Advisor

Azure Advisor에서 비용에 대한 추천 정보를 얻을 수 있다.

Management + governance > Advisor 로 진입

활용 예시

Reduce costs by eliminating unprovisioned Azure ExpressRoute : Not provisioned for more than one month

Buy reserved instances to save money over pay-as you-go : review VM usage over the last 30 days could save money in the future by purchasing reserved instances

Right-size or shutdown underutilized virtual machines : monitor VM usage for 14 days and identifies underutilized VM

4. Understand Azure Pricing and Support

Azure 비용 최소화에 도움되는 방법

Perform cost analyses : Azure Pricing 및 TCO 계산기로 비용 분석

Monitor usage with Azure Advisor : 비용 권장 사항 확인

Use spending limits : credit 사용으로 월별 지출 한도 설정 가능

Use Azure Reservations : 1~3년 선 구매 형태를 활용하면 비용 절감 가능(RI : Reserved Instance) CapEx 처럼 미리 비용을 선 지불 하면 최대 72%까지 가격 할인을 해준다고 함.

Choose low-cost locations and regions : region 선택이 자유로울 경우 최저 비용을 지원하는 region 선택

Apply tags to identify cost owners : 태그를 활용하여 비용 소비 모니터

Azure credits : App Service, VM, DB, Container 등 새로운 기능 사용 시 Credit 사용 가능

Deallocate virtual machines in off hours : 업무 시간 이후에는 시스템 종료되도록 설정 가능

Migrate to PaaS or SaaS services : IaaS로 시작해보고 추후 가능하다면 PaaS나 SaaS로 전환

4. Understand Azure Pricing and Support

Azure Cost Management

Azure Advisor보다 한단계 업그레이드된 기능을 제공

another free, built-in Azure tool that can be used to gain greater insights into where your cloud money is going. You can see **historical breakdowns of what services you are spending** your money on and how it is tracking against budgets that you have set. You can set budgets, schedule reports, and analyze your cost areas.

Support options available with Azure

지원 계획 옵션

청구 및 subscription 지원에 대한 무료 액세스

Azure 제품 및 서비스 설명서

온라인 자가 도움말 문서

커뮤니티 지원 포럼

추가 학습 자료

MS 공식 Learn 웹 페이지 (영문, 한글)

<https://docs.microsoft.com/en-ie/learn/paths/azure-fundamentals/>

MS 공식 실습 페이지 (영문)

<https://microsoftlearning.github.io/AZ-900T0x-MicrosoftAzureFundamentals/>

MS 공식 가이드북 (영문)

모바일 버전 - https://download.microsoft.com/download/6/6/2/662DD05E-BAD7-46EF-9431-135F9BAE6332/9781509302963_Microsoft%20Azure%20Essentials%20Fundamentals%20of%20Azure%202nd%20ed%20mobile.pdf

PC 버전 - <https://download.microsoft.com/DOWNLOAD/2/C/A/2CA4DC8E-021C-4D56-8529-DF4F71FF4A1B/9780735697225.PDF>

한글 무료 동영상 강의

<https://educast.com/course/other-cert/ZB88>

Exam Dump

<https://www.testpassport.com/AZ-900-exam.html>

<https://quizizz.com/admin/quiz/5daee79cb52627001a14fb91/azure-pb>

<https://quizizz.com/admin/quiz/5c9b860379a3d3001abd5181/azure>

<https://www.exam-answer.com/microsoft/az-900>

<https://vceguide.com/microsoft/az-900-microsoft-azure-fundamentals/>

<https://www.examttopics.com/exams/microsoft/az-900/view/1/>