Розподілені системи та хмарні технології

Що таке "хмара" і хмарні технології
Класифікація хмар

Визначення

- **Хмарні обчислення** (англ. *cloud computing*) або скорочено **хмара** — модель забезпечення повсюдного та зручного **доступу на вимогу** через мережу до **спільного пулу обчислювальних ресурсів**, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), і які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера.

Переваги хмар

- Масштабованість та гнучкість
- Безпека
- Зменшення затрат на підтримку інфраструктури
- Екологічність (уникнення використання надлишкових ресурсів)
- Regulatory compliance (GDPR і т.д.)
- Забезпечення близькості до користувача, реплікація
- Швидкість розгортання
- Висока доступність
- Pay-as-you-go (ви платите тільки за те, що використовуєте)
- Використання ресурсів в залежності від навантаження

Недоліки хмар

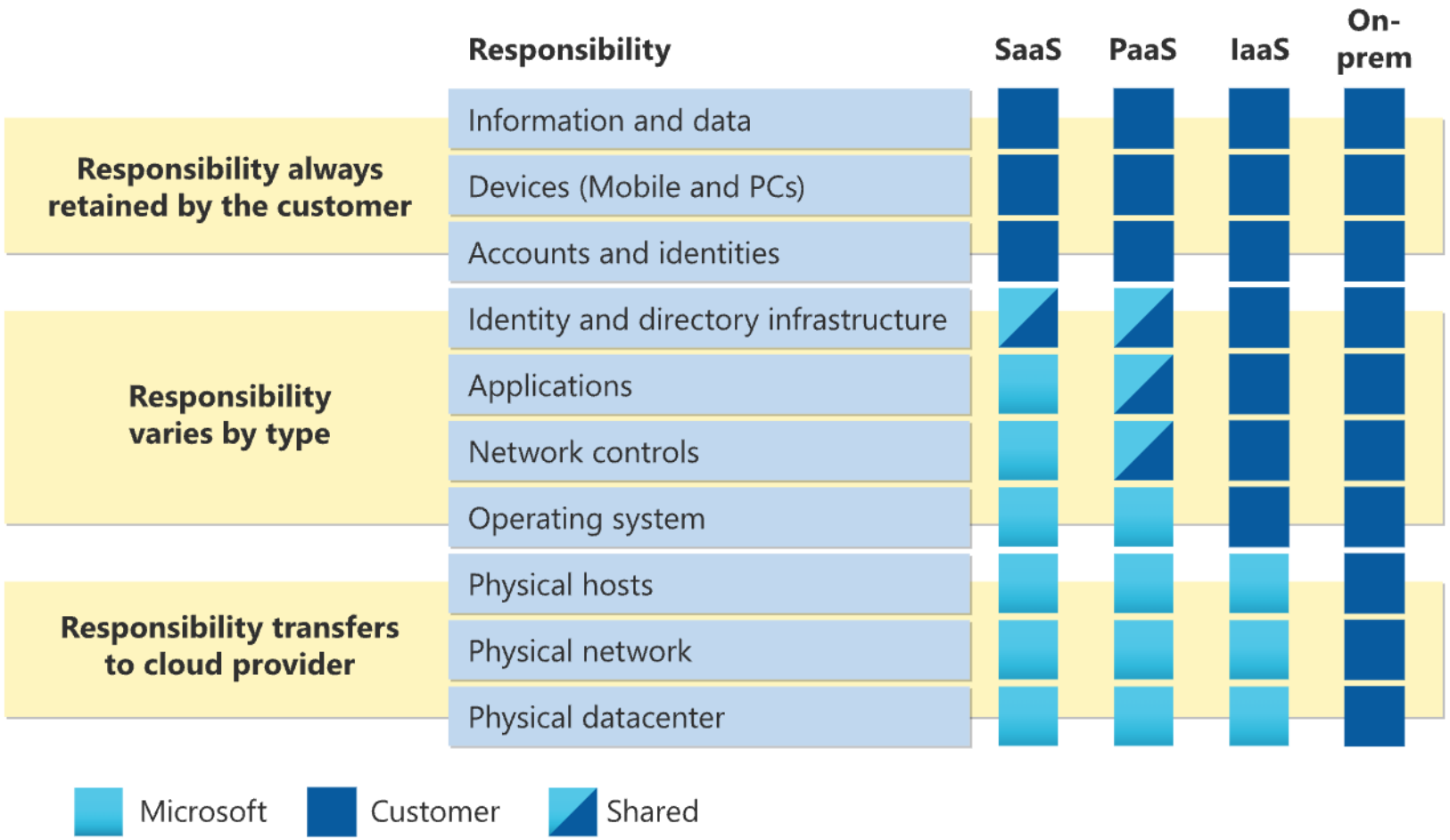
- Відсутність контролю за даними, недостатня гнучкість
- Вартість інфраструктури (https://azure.microsoft.com/en-us/pricing/calculator/), приховані витрати
- Vendor-lock і складність міграції між хмарами при використанні специфічних ресурсів
- Залежність від інтернет-підключення

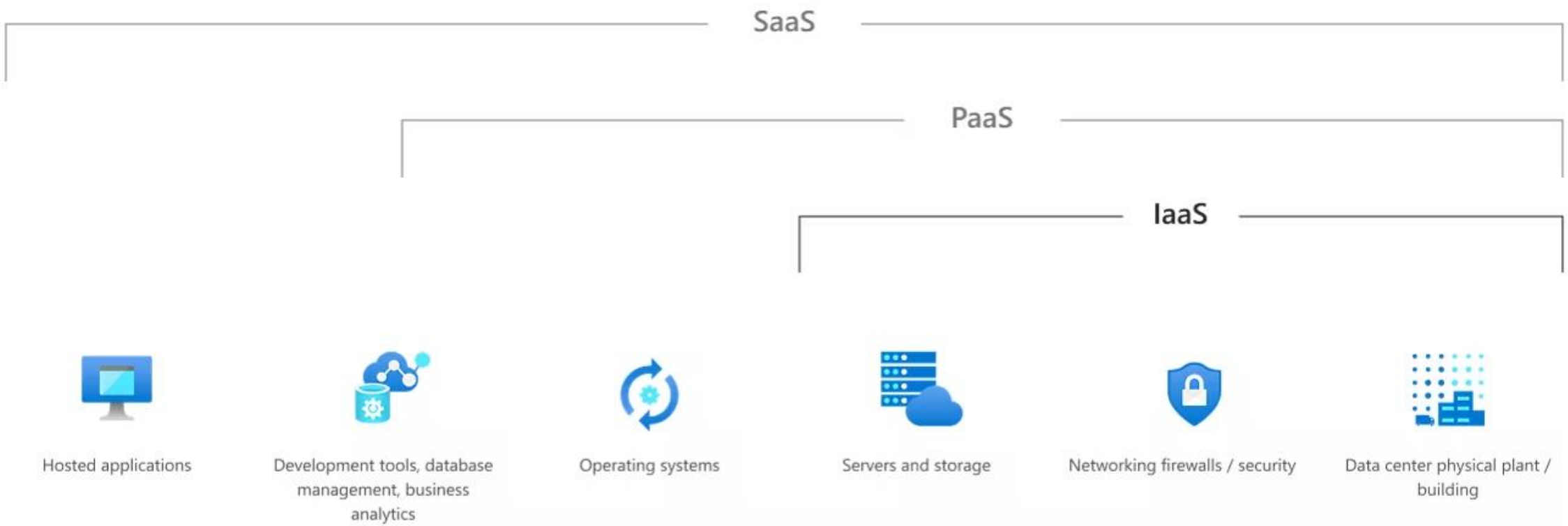
Види хмарних обчислень (Основні групи послуг)

Інфраструктура як сервіс
(Infrastructure as a Service, IaaS)

Платформа як сервіс
(Platform as a Service, PaaS)

Програмне забезпечення як сервіс
(Software as a Service, SaaS)


Responsibility
SaaS
PaaS
IaaS
On-prem
Responsibility always retained by the customer
Information and data
Devices (Mobile and PCs)
Accounts and identities
Responsibility varies by type
Identity and directory infrastructure
Applications
Network controls
Operating system
Responsibility transfers to cloud provider
Physical hosts
Physical network
Physical datacenter
Microsoft
Customer
Shared



Infrastructure as a Service (IaaS)
Інфраструктура як сервіс

- IaaS - це тип послуги хмарних обчислень, який пропонує необхідні обчислювальні ресурси, сховища та мережеві ресурси на вимогу, за принципом «pay-as-you-go»
- Апаратні засоби (сервери, системи зберігання даних, клієнтські системи, мережеве обладнання)
- Операційні системи та системне ПЗ(засоби віртуалізації, автоматизації, основні засоби керування ресурсами)
- Дата центри, будівля ЦОД

IaaS – Висновки

- IaaS позбавляє необхідності підтримки складних інфраструктур центрів обробки даних, клієнтських і мережевих інфраструктур, а також дозволяє зменшити пов'язані з цим капітальні і поточні витрати. Можлива й додаткова економія, якщо послуги надаються в рамках інфраструктури спільного використання

Приклади IaaS

Related Azure IaaS services and products

Azure IaaS

Azure Virtual Machines

Azure Disk Storage

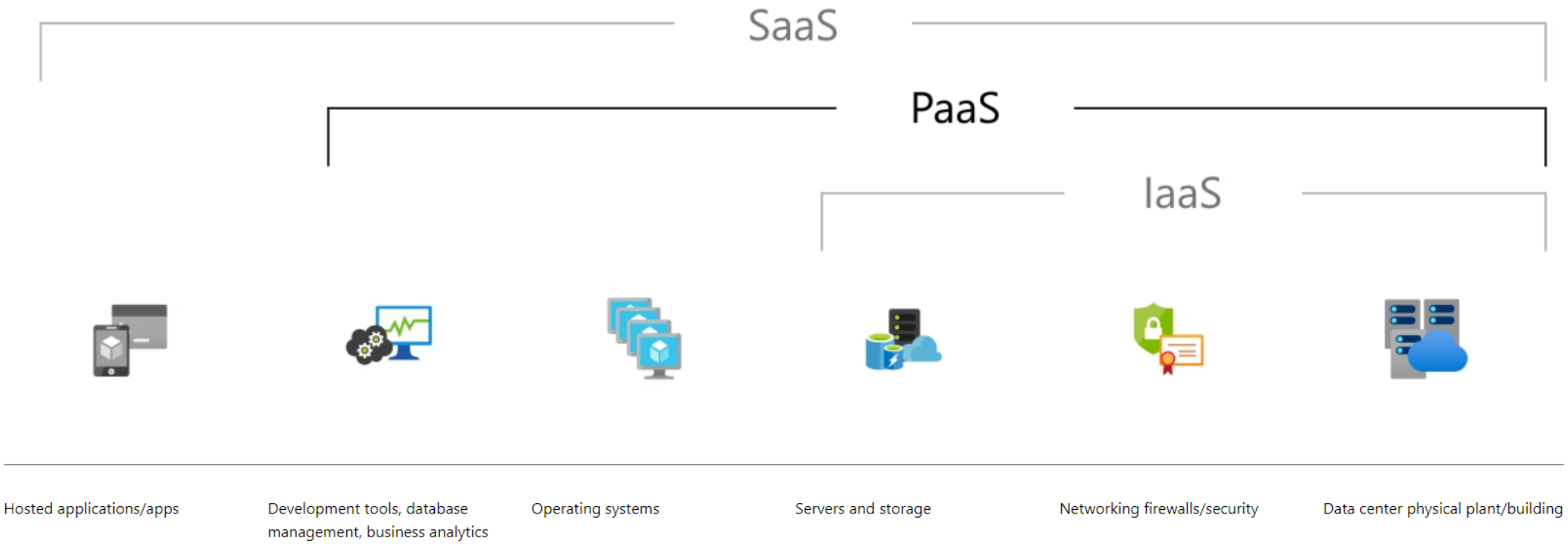
Azure networking

Business-critical applications

Hybrid cloud solutions

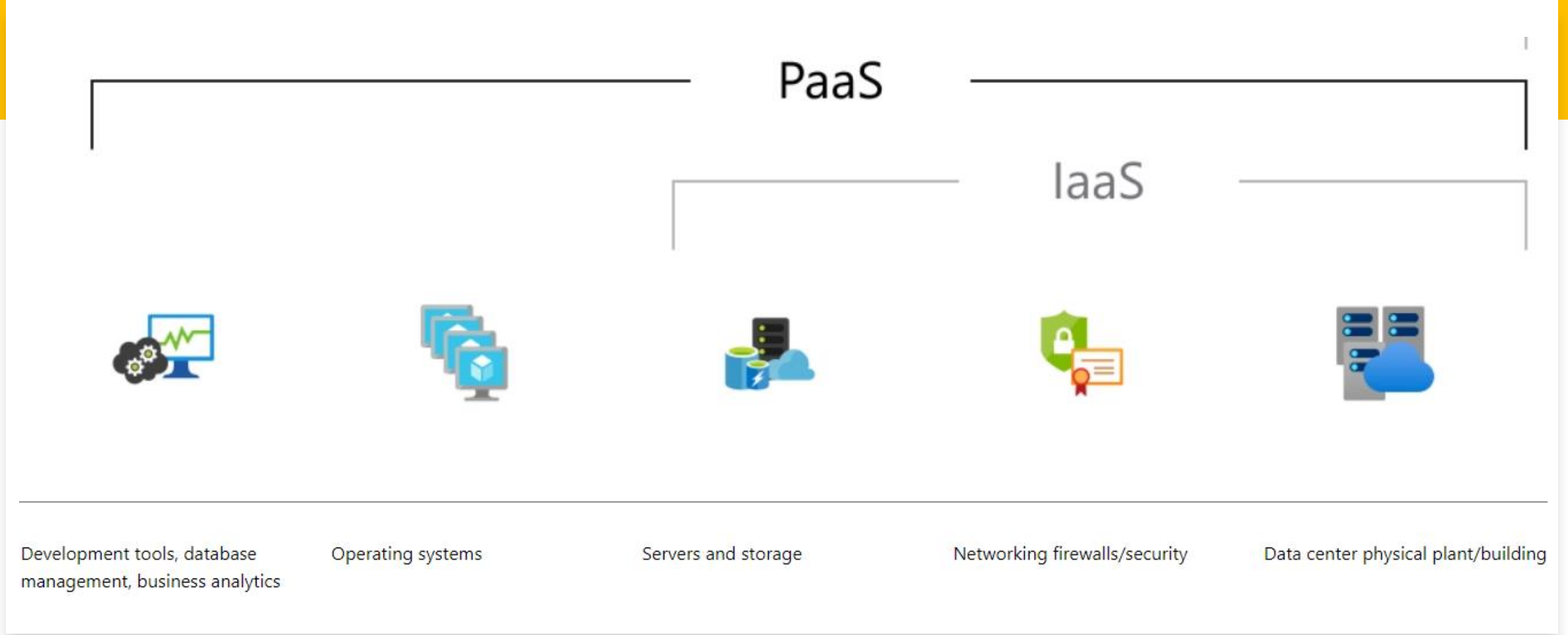
Management and governance

Security



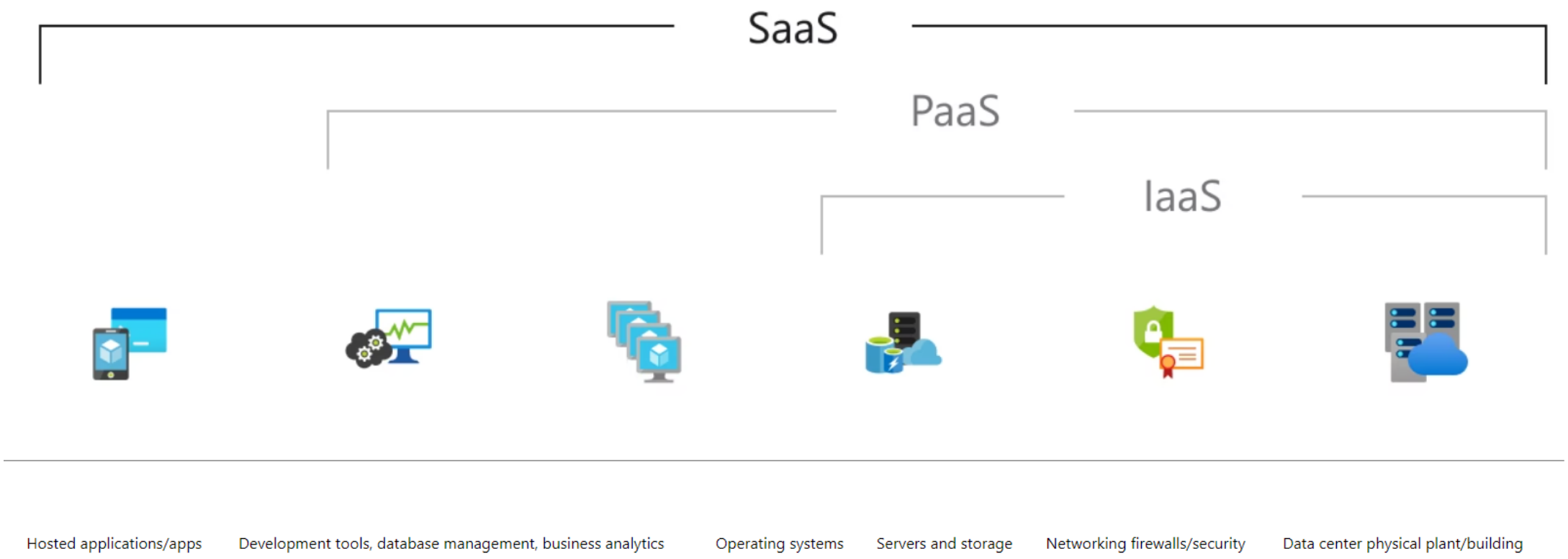
Platform as a Service (PaaS)
Платформа як сервіс

- PaaS надає спеціальну платформу для розробки, тестування та розгортання програмного забезпечення та застосунків. Основна ідея PaaS полягає в тому, щоб спростити розробку та управління застосунками, надаючи розробникам доступ до середовища, інструментів та ресурсів, необхідних для створення додатків, без необхідності прямої взаємодії з фізичною інфраструктурою або операційними системами.
- PaaS забезпечує повний життєвий цикл застосунку: розробка, тестування, розгортання, моніторинг і підтримка



PaaS – Висновки

- PaaS дозволяє підняти швидкість розробки і розгортання, що є критичним в нашій ринковій економіці. При цьому зберігається гнучкість. Корпоративні рішення які починають розроблятися в 2020х роках здебільшого базуються саме на PaaS. При цьому ми не контролюємо життєвий цикл платформи (оновлення і тд.)

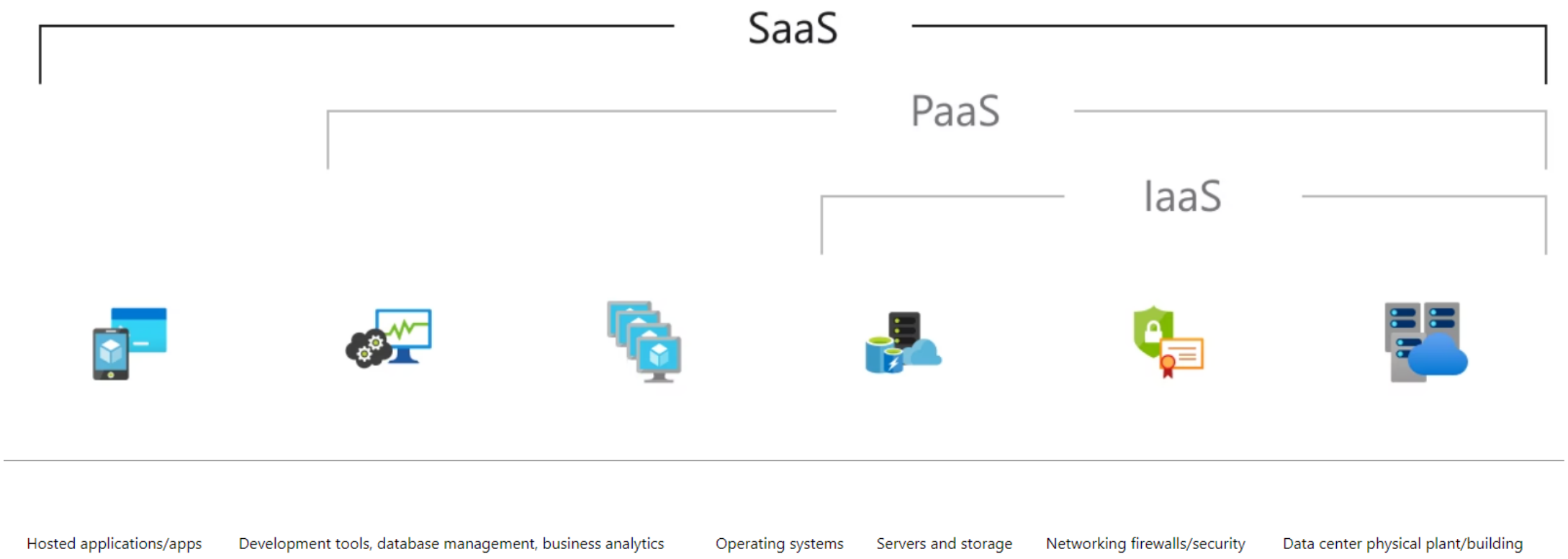


Software as a Service (SaaS) Програмне забезпечення як сервіс

- SaaS – це модель пропозиції програмного забезпечення споживачеві, при якій постачальник розробляє веб-додаток розміщує і управляє ним(самостійно або через третіх осіб) з метою і можливістю використання замовниками через інтернет.
- Замовники платять не за володіння програмним забезпеченням як таким, а за його використання(API, Web, веб-служби)

SaaS vs Додаток/застосунок(Hosted application)

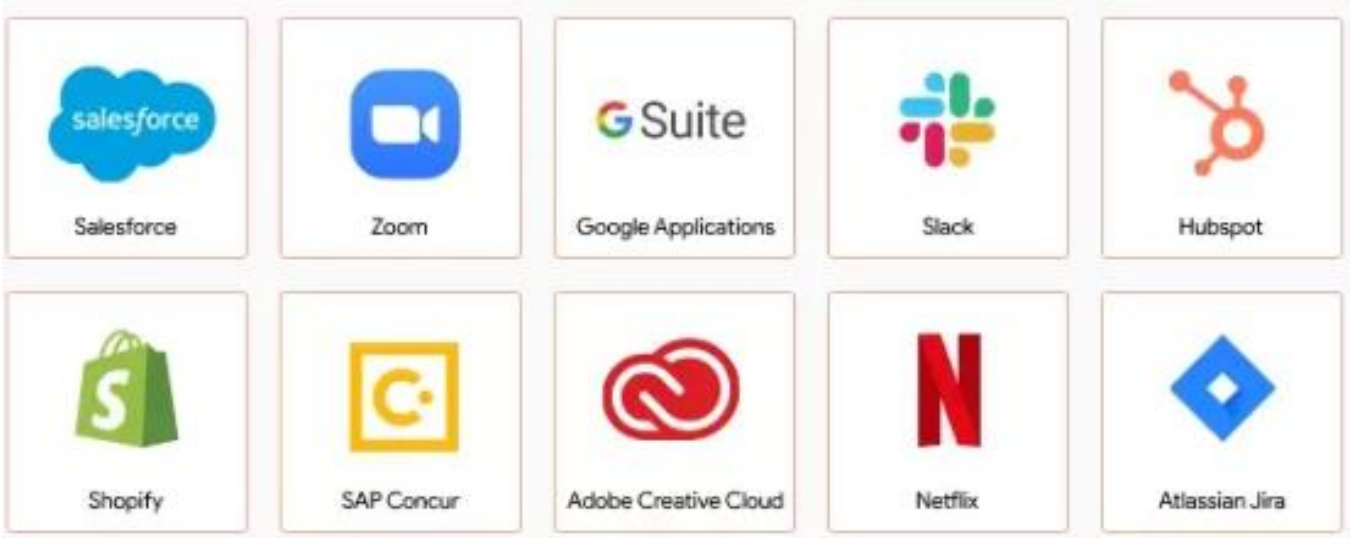
- SaaS продає вирішення певної проблеми і знаходиться на рівень абстракції вище за програмую Фактично різниця в моделі поширення та монетизації.
- Купити гру в Steam і пограти в неї – це застосунок, ми розгортаємо його на своїх ресурсах
- Хмарний геймінг – це SaaS, провайдер значною мірою вирішує питання ресурсів і пропонує вирішення задачі «погратися» на період проплати



SaaS - Висновки

- Переваги: швидка інтеграція, низька вартість підтримки, автоматичні оновлення
- Недоліки: залежність від SaaS партнера, недостатня гнучкість, автоматичні оновлення

Приклади SaaS



Гібриди

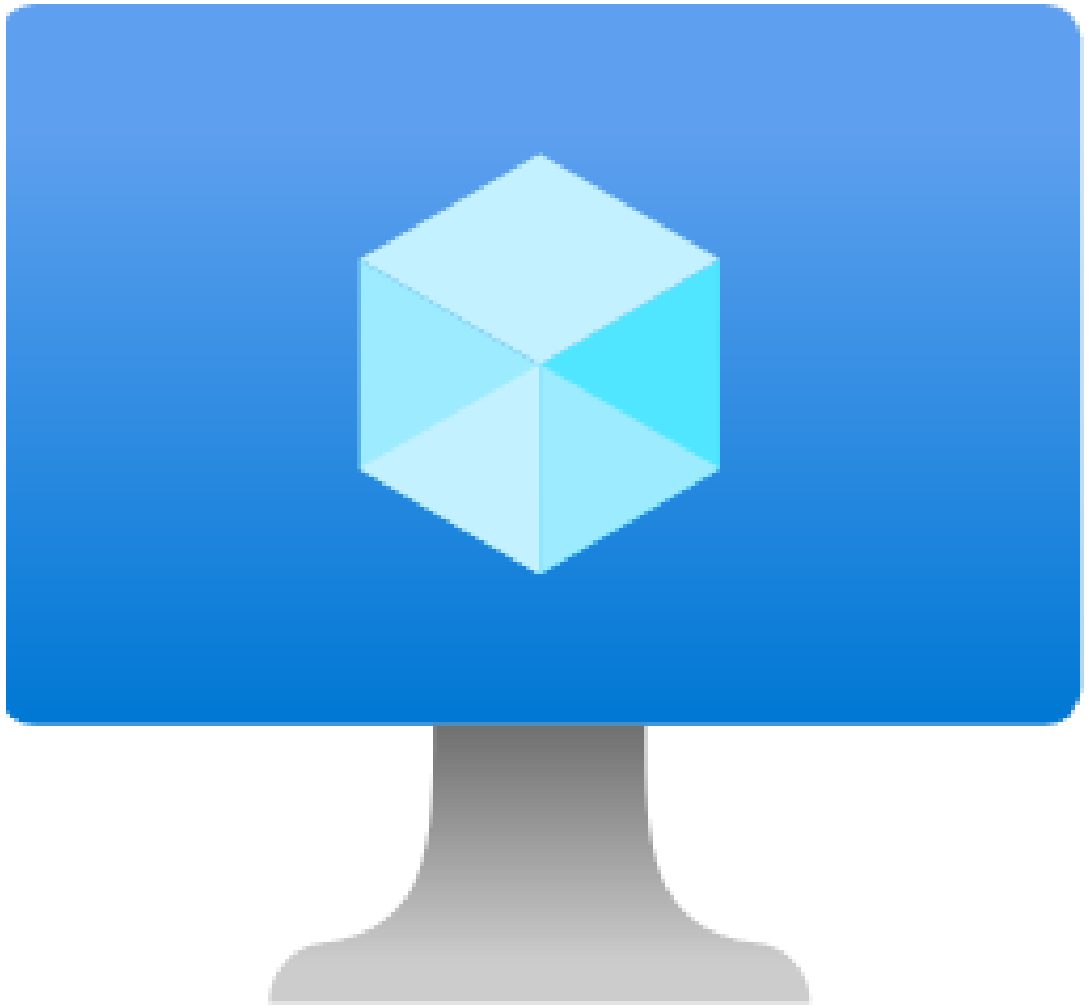
- IaaS+PaaS – IaaS для legacy інфраструктури, PaaS для нових компонентів
- PaaS+SaaS – IBM Whatsons IoT hub, з одного боку інтеграційна платформа, з іншого AI для аналізу і тд.

Хмарні технології

Azure VM

Azure VM

- **Віртуальні машини Azure** - це сервіс платформи Azure, який надає масштабовані обчислювальні ресурси на вимогу через віртуальні машини, і вони можуть бути налаштовані та управлятися через Інтернет. Вони надають користувачам можливість запуску та управління власними віртуальними серверами для виконання різноманітних завдань. Azure надає широкий вибір розмірів та конфігурацій віртуальних машин, що дозволяє вибрати найбільш підходящий варіант для конкретних потреб.



Основні направлення використання Azure VM

Хостинг веб-сайтів та веб-додатків: Azure VM дозволяє створювати віртуальні сервери для розгортання та управління веб-сайтами та веб-додатками, що дозволяє масштабувати їх залежно від навантаження.

Розробка та тестування програм: Розробники можуть створювати власні розробочі середовища на Azure VM для розробки та відлагодження програм.

Бази даних: Azure VM може бути використана для розгортання та управління базами даних, включаючи Microsoft SQL Server, MySQL, PostgreSQL та інші.

Аналіз даних: Використовуючи великі обсяги обчислювальних ресурсів в Azure VM, можна виконувати складні обчислення та аналіз даних.

Віртуалізація: Azure VM дозволяє створювати віртуальні ізольовані середовища для запуску різних операційних систем і додатків.

Додатки для великих даних: Для обробки та аналізу великих обсягів даних можна використовувати Azure VM в поєднанні зі службами, такими як Azure HDInsight.

Забезпечення відмовостійкості та відновлення після аварій: Azure VM дозволяє створювати резервні копії та відновлювати віртуальні машини для забезпечення високої доступності і відновлення в разі аварії.

Робочі групи та обчислення віртуальних робочих столів: VM можуть бути використані для надання користувачам віддаленого доступу до робочих столів та програм через Інтернет.

Ігрова інфраструктура: Azure VM може бути використана для розгортання ігрових серверів та інфраструктури для онлайн-ігор.

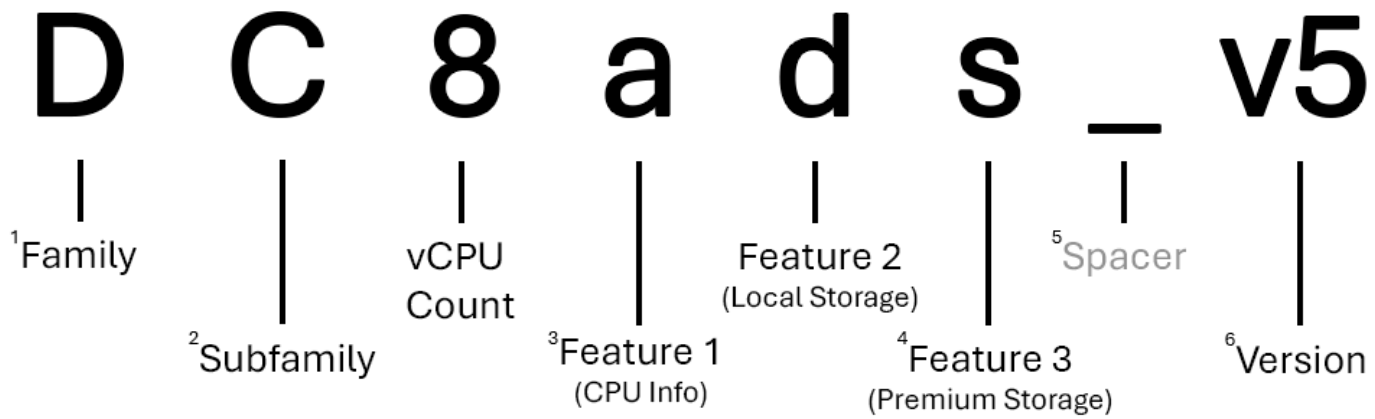
Інфраструктура для штучного інтелекту та машинного навчання: Azure VM дозволяє надавати обчислювальні ресурси для тренування та розгортання моделей штучного інтелекту та машинного навчання.


54 regions worldwide
140 available in 140 countries
West US 2
West Central US
West US
US Gov Arizona
South Central US
US Gov Texas
US Gov Iowa
Central US
US Gov Virginia
US DoD Central
Canada East
Canada Central
North Central US
US DoD East
East US
East US 2
Norway West
Norway East
West Europe
Germany West Central
UK South
Germany North
North Europe
Germany Northeast
UK West
Germany Central
France Central
Switzerland North
France South
Switzerland West
China North
China North 2
Korea Central
Korea South
Japan East
Japan West
China East 2
China East
East Asia
UAE North
UAE Central
West India
Central India
South India
Southeast Asia
Brazil South
South Africa North
South Africa West
Australia East
Australia Central
Available region
Announced region
Availability Zones

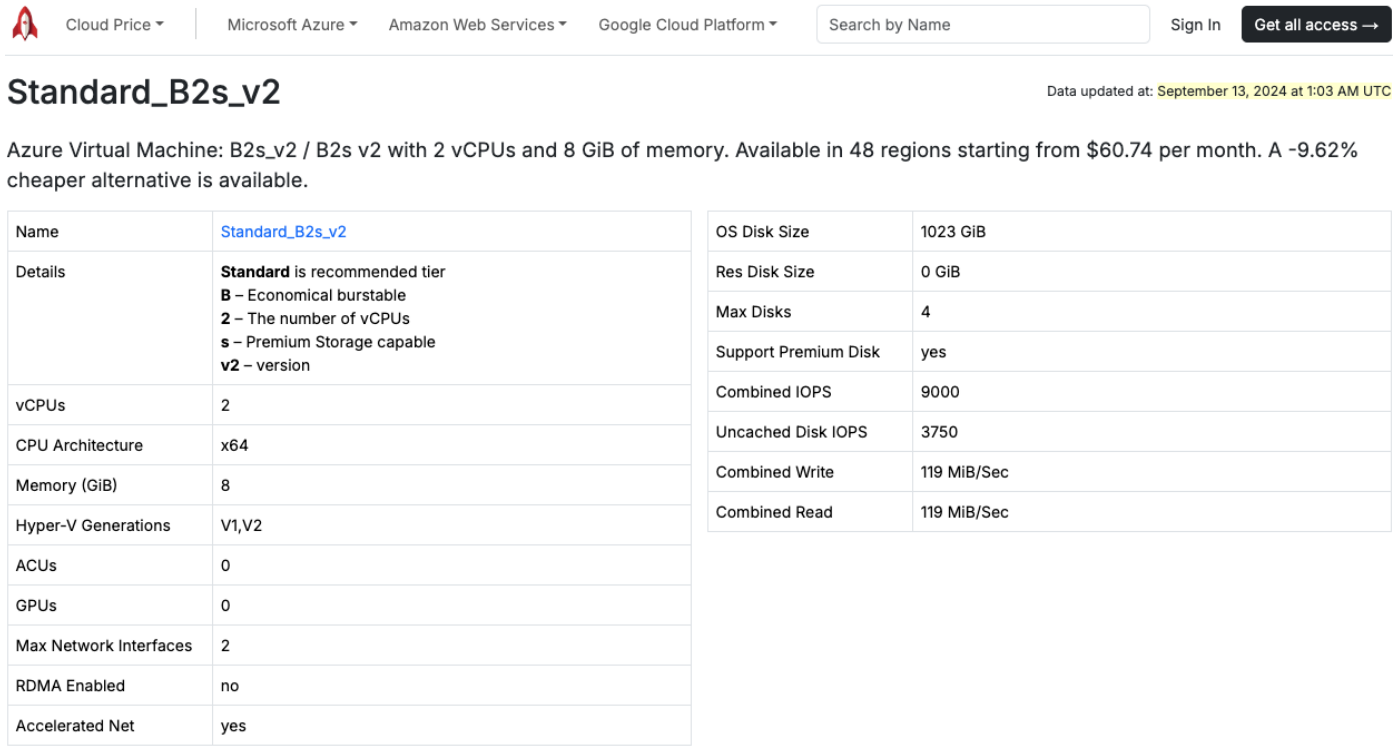
Розміри віртуальних машин

Type	Sizes	Description
General purpose	Dsv3, Dv3, DSv2, Dv2, DS, D, Av2, A0-7	Balanced CPU-to-memory. Ideal for dev/test and small to medium applications and data solutions.
Compute optimized	Fs, F	High CPU-to-memory. Good for medium-traffic applications, network appliances, and batch processes.
Memory optimized	Esv3, Ev3, M, GS, G, DSv2, DS, Dv2, D	High memory-to-core. Great for relational databases, medium to large caches, and in-memory analytics.
Storage optimized	Ls	High disk throughput and IO. Ideal for big data, SQL, and NoSQL databases.
GPU optimized	NV, NC	Specialized VMs targeted for heavy graphic rendering and video editing.
High performance	H, A8-11	Our most powerful CPU VMs with optional high-throughput network interfaces (RDMA).

Розміри віртуальних машин



Розміри віртуальних машин



Cloud Price | Microsoft Azure | Amazon Web Services | Google Cloud Platform | Search by Name | Sign In | Get all access →

Standard_B2s_v2

Data updated at: September 13, 2024 at 1:03 AM UTC

Azure Virtual Machine: B2s_v2 / B2s v2 with 2 vCPUs and 8 GiB of memory. Available in 48 regions starting from $60.74 per month. A -9.62% cheaper alternative is available.

Name	Standard_B2s_v2
Details	**Standard** is recommended tier **B** – Economical burstable **2** – The number of vCPUs **s** – Premium Storage capable **v2** – version
vCPUs	2
CPU Architecture	x64
Memory (GiB)	8
Hyper-V Generations	V1,V2
ACUs	0
GPUs	0
Max Network Interfaces	2
RDMA Enabled	no
Accelerated Net	yes

OS Disk Size	1023 GiB
Res Disk Size	0 GiB
Max Disks	4
Support Premium Disk	yes
Combined IOPS	9000
Uncached Disk IOPS	3750
Combined Write	119 MiB/Sec
Combined Read	119 MiB/Sec

Обмеження кількості віртуальних машин

Квоти ресурсів: У вас є обмеження на кількість ресурсів, які ви можете створити у межах своєї підписки Azure.

Тип рахунку: Тип вашого рахунку (наприклад, безкоштовний пробний рахунок, платний рахунок) також впливає на кількість доступних ресурсів та їх обмеження.

Регіон: Кожен регіон Azure має власні обмеження на ресурси, і ці обмеження можуть відрізнятися від регіону до регіону.

Розмір віртуальних машин: Розмір та конфігурація ваших віртуальних машин також може вплинути на обмеження. Деякі розміри машин можуть бути обмежені залежно від доступних ресурсів у вибраному регіоні.

Інші фактори: Ваша активність в Azure, наявність резервованих екземплярів, обрані служби та функції також можуть вплинути на кількість доступних ресурсів.

*стандартна квота VM це 20 екземплярів на одну підписку. Ці квоти можна змінити, подавши запит на збільшення обмежень або вибираючи більш високий рівень підписки.

Операційні системи Azure VM

Windows Server: Azure пропонує різні версії Windows Server, такі як Windows Server 2022, Windows Server 2019, і багато інших.

Linux: Ви можете встановлювати різні дистрибутиви Linux, такі як Ubuntu, CentOS, Debian, Red Hat Enterprise Linux, SUSE Linux Enterprise, та інші.

FreeBSD: FreeBSD є ще однією операційною системою, яку можна використовувати на Azure VM.

Oracle Linux: Якщо вам потрібно використовувати Oracle Linux для ваших додатків, ви можете розгортати його на Azure VM.

SAP HANA: Для підтримки SAP HANA, Azure надає спеціально налаштовані віртуальні машини.

Інші операційні системи: Крім перерахованих вище, є багато інших операційних систем, доступних для розгортання на Azure VM, включаючи спеціалізовані ОС та варіанти.

*Можливість завантаження свого образу для VM

Способи розгортання віртуальних машин

Панель управління Azure (Azure Portal):

- Це веб-інтерфейс для управління ресурсами Azure.
- Ви можете створювати VM, обирати операційну систему, конфігурацію та регіон, в якому вони будуть розгортатися.
- Цей метод найпростіший для початківців.

Azure CLI (Command-Line Interface):

- Ви можете використовувати командний рядок для створення і керування VM з використанням Azure CLI.
- Цей метод дозволяє автоматизувати розгортання та конфігурацію VM за допомогою сценаріїв.

Azure PowerShell:

- Аналогічно до Azure CLI, Azure PowerShell дозволяє створювати та управляти VM за допомогою команд у командному рядку.
- Це особливо корисно для адміністраторів, які вже використовують PowerShell для автоматизації завдань.

Шаблони ARM (Azure Resource Manager):

- Ви можете створювати шаблони ARM, що описують ресурси Azure, включаючи VM, їхню конфігурацію та залежності.
- Шаблони ARM дозволяють вам визначити інфраструктуру як код і автоматизувати розгортання.

Azure DevTest Labs:

- Це сервіс, призначений для створення та керування виробничими і тестовими середовищами, включаючи VM.
- Ви можете швидко створювати VM для розробки та тестування програм.

Засоби інтеграції та розгортання (CI/CD):

- Ви можете використовувати інструменти для неперервної інтеграції та неперервної доставки (CI/CD), такі як Azure DevOps, Jenkins, або GitLab CI/CD, для автоматичного розгортання VM.

Azure Marketplace:

- Ви можете вибрати готові образи VM та розгортати їх з Azure Marketplace, де є велика кількість готових рішень та стеків програмного забезпечення.

Інші інструменти і SDK:

- Azure також підтримує розгортання VM з використанням інших інструментів та SDK, таких як Terraform, Ansible, або власні скрипти на різних мовах програмування.

Віртуальні мережі (Virtual Networks або VNETs)

Ізоляція та сегментація: Віртуальні мережі дозволяють створювати окремі мережеві сегменти для різних застосунків або сервісів. Це допомагає уникнути зіткнень мережевого трафіку і забезпечити безпеку і приватність даних.

Підмережі (Subnets): Ви можете поділити свою віртуальну мережу на підмережі для кращого управління IP-адресами і ресурсами. Підмережі можуть мати свої правила маршрутизації та забезпечувати доступ до різних VM.

Захист мережі: Azure надає можливість налаштовувати правила мережевої безпеки (Network Security Groups або NSG) для кожного віртуального інтерфейсу машини. NSG дозволяють контролювати вхідний та вихідний трафік, який надходить до VM.

Віддалений доступ: За допомогою віртуальних мереж можна налаштувати віддалений доступ до VM, такий як віддалене управління через SSH або RDP.

VPN та ExpressRoute: Azure дозволяє підключати віртуальні мережі до існуючих мереж корпорації за допомогою VPN-з'єднань або ExpressRoute для створення гібридних мереж.

Мережеві сервіси: Azure пропонує різні мережеві служби, такі як Azure Load Balancer для розподілення трафіку, Azure Application Gateway для керування веб-трафіком і Azure Firewall для забезпечення безпеки мережі.

IPv6 підтримка: Azure підтримує IPv6, що дозволяє використовувати цю нову версію протоколу для вашого мережевого трафіку.

Планування маршрутів: Ви можете налаштовувати правила маршрутизації для мережі, які дозволяють визначити напрямок трафіку і з'єднання між підмережами та різними ресурсами.

Мережеві адаптери (Network Adapters)

- **Внутрішні мережеві адаптери**: Всі віртуальні машини в Azure мають внутрішні мережеві адаптери, які дозволяють взаємодіяти з іншими VM в межах тієї ж віртуальної мережі (VNET). Це надає можливість комунікації між VM на одному і тому ж VNET.
- **Зовнішні мережеві адаптери**: Azure VM також може мати зовнішні мережеві адаптери, які дозволяють з'єднувати VM з інтернетом або іншими зовнішніми мережами. Це потрібно для забезпечення доступу до VM з інших мереж або з інтернету, наприклад, через RDP або SSH.
- **IP-адреси**: Кожний мережевий адаптер може мати одну або більше IP-адрес, які визначаються для віртуальних машин в Azure. Це дозволяє ідентифікувати та адресувати VM в мережі.
- **Діапазони IP-адрес**: Ви можете налаштовувати діапазони IP-адрес для мережевих адаптерів у віртуальних мережах Azure, що дозволяє контролювати доступ до VM та надавати їм статичні або динамічні IP-адреси.
- **Маршрутизація та маршрути**: Мережеві адаптери вирішують завдання маршрутизації, визначаючи спосіб, яким трафік повинен бути направлений між VM та іншими ресурсами.
- **Мережева безпека**: Мережеві адаптери можуть бути налаштовані з правилами мережевої безпеки, такими як Network Security Groups (NSG), для керування трафіком і забезпечення безпеки мережі.
- **Віддалений доступ**: За допомогою мережевих адаптерів можна налаштовувати віддалений доступ до віртуальних машин, такий як RDP або SSH, для віддаленого керування та адміністрування.

IP-адреси (Internet Protocol addresses)

IPv4 (Internet Protocol version 4): Це найбільш поширений стандарт IP-адрес у світі. IPv4 адреси складаються з 32-бітних чисел, поділених на 4 октети (кожен октет представляє собою 8 бітів) і записуються у форматі, наприклад, "192.168.1.1". Проте через обмежену кількість доступних IPv4 адрес виникла необхідність в переході на IPv6.

IPv6 (Internet Protocol version 6): Це новіший стандарт IP-адрес, який розроблений для забезпечення великої кількості унікальних адрес. IPv6 використовує 128 бітів для представлення адреси, що дає величезний резерв доступних адрес. IPv6 адреси зазвичай записуються у форматі, наприклад, "2001:0db8:85a3:0000:0000:8a2e:0370:7334".

Віртуальна мережа (Virtual Network або VNET) та підмережа (Subnet)

Віртуальна мережа (VNET):

Віртуальна мережа (VNET) є логічним сегментом мережі в хмарному середовищі, який може бути контрольований та налаштований користувачем.

VNET визначає межі вашої мережі в хмарному середовищі Azure або інших хмарних платформах. Вона може бути використана для групування та управління вашими віртуальними машинами, базами даних, веб-сервісами та іншими ресурсами в одній мережі.

VNET також визначає діапазон IP-адрес, які можуть бути використані у межах цієї мережі.

Підмережа (Subnet):

Підмережа (Subnet) є підрозділом віртуальної мережі (VNET). Вона представляє собою додатковий рівень сегментації у межах VNET.

Підмережі дозволяють розділити VNET на менші логічні сегменти для кращого управління ресурсами та налаштуванням доступу та безпеки.

Кожна підмережа в межах VNET має свій власний діапазон IP-адрес, який визначається в межах діапазону IP-адрес VNET. Це дозволяє вам призначити IP-адреси ресурсам у мережі та контролювати комунікацію між різними підмережами.

Підмережі використовуються для поділу VNET на логічні зони або категорії ресурсів. Наприклад, ви можете створити підмережу для веб-серверів та окрему підмережу для баз даних, і контролювати доступ між ними.

Групи безпеки мережі (Network Security Groups або NSG)

Фільтрація трафіку: NSG дозволяють вам визначити правила фільтрації трафіку на основі джерела, призначення, портів та протоколів. Ви можете встановлювати правила для блокування або дозволу трафіку в залежності від вашого потреб.

Діапазони IP-адрес: Ви можете визначити діапазони дозволених IP-адрес для кожного правила, що дозволяє обмежувати доступ до ресурсів з конкретних IP-адрес або мереж.

Правила безпеки: NSG мають набір правил безпеки, які ви можете налаштовувати для забезпечення безпеки вашої мережі. Це може включати блокування портів, налаштування віддаленого доступу та інші заходи.

Пріоритети правил: Кожне правило в NSG має пріоритет, який визначає порядок застосування правил. Це дозволяє вам контролювати, яке правило застосовується, якщо декілька правил відповідають одному пакету.

Асоціація з ресурсами: NSG можуть бути асоційовані з віртуальними машинами або підмережами. Це дозволяє вам визначити правила безпеки для конкретних ресурсів або сегментів мережі.

Моніторинг і журналювання: Azure надає можливість моніторити та журналювати мережевий трафік, що пройшов через NSG, для аналізу безпеки та виявлення інцидентів.

Захист від DDoS-атак: NSG можуть допомогти вам забезпечити захист вашої мережі від розподіленого відмови в обслуговуванні (DDoS) за допомогою налаштувань та правил безпеки.

Зони доступності (Availability Zones)

1. **Висока доступність**: Завдяки фізичному розділенню та незалежності інфраструктури між зонами доступності, ви можете забезпечити високий рівень доступності для вашого додатку або служби. Це означає, що навіть якщо одна зона недоступна через відмову або обслуговування, інші зони залишаються доступними.
2. **Резервне копіювання даних**: Зони доступності можуть використовувати для розміщення резервних копій ваших даних та додатків, забезпечуючи їх стійкість до відмов та можливість відновлення.
3. **Зменшення ризику відмов**: Розміщення різних компонентів додатку або сервісу у різних зонах доступності допомагає зменшити ризик відмов та забезпечити більш високий рівень стійкості.
4. **Балансування навантаження**: Ви можете використовувати зони доступності для розміщення компонентів своєї інфраструктури та автоматичного балансування навантаження між ними для оптимізації продуктивності та доступності.
5. **Розташування близько до клієнтів**: Зони доступності дозволяють розміщувати ваші додатки та дані близько до вашої аудиторії, що може покращити швидкість доступу до ресурсів.
6. **Масштабованість**: Зони доступності розширюють можливості масштабування вашого додатку або сервісу, дозволяючи легко додавати ресурси у різних зонах для забезпечення високої продуктивності.

Зони доступності (Availability Zones)

Можливості масштабування віртуальних машин

Вертикальне масштабування (Scaling Up/Down):

- Вертикальне масштабування, полягає в зміні розміру віртуальної машини, наприклад, збільшення кількості процесорів або обсягу пам'яті.

Горизонтальне масштабування (Scaling Out/In):

- Горизонтальне масштабування означає додавання або видалення додаткових віртуальних машин для обробки навантаження.

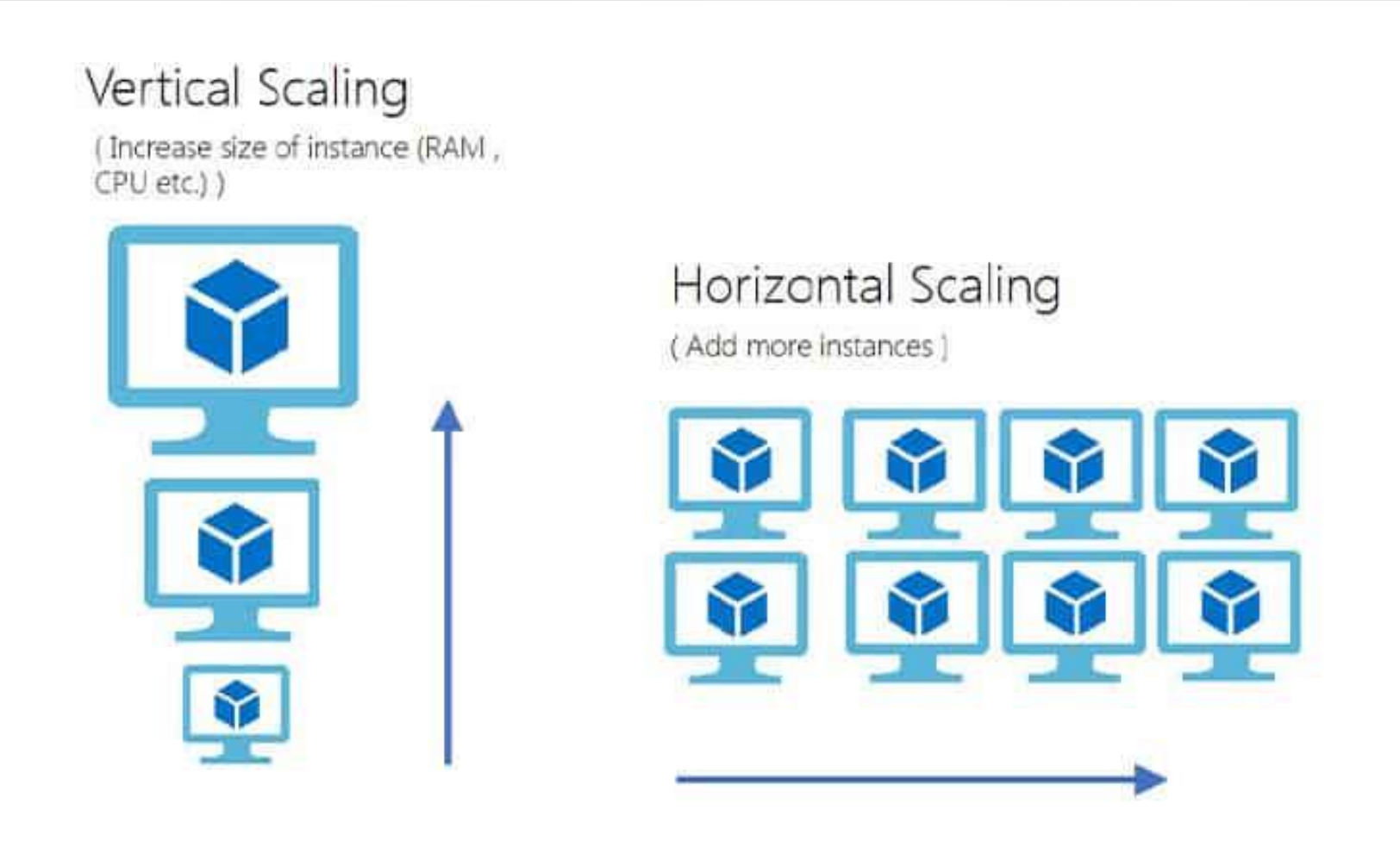
Azure Virtual Machine Scale Sets:

- Azure Virtual Machine Scale Sets (VMSS) - це служба Azure, яка дозволяє автоматично створювати та керувати групами віртуальних машин з можливістю автоматичного горизонтального масштабування.

Azure Auto Scaling:

- Azure Auto Scaling дозволяє автоматично масштабувати віртуальні машини або інші ресурси в залежності від поточного навантаження або метрик моніторингу.

Можливості масштабування віртуальних машин



Групи доступності (Availability Sets)

Фізична і логічна роздільність: Групи доступності розділяють ваші віртуальні машини на фізично відокремлені розташування (фізичні сервери) і логічні розташування (зони в одному регіоні). Це забезпечує високу доступність навіть в разі відмови на одному фізичному сервері або в одній зоні.

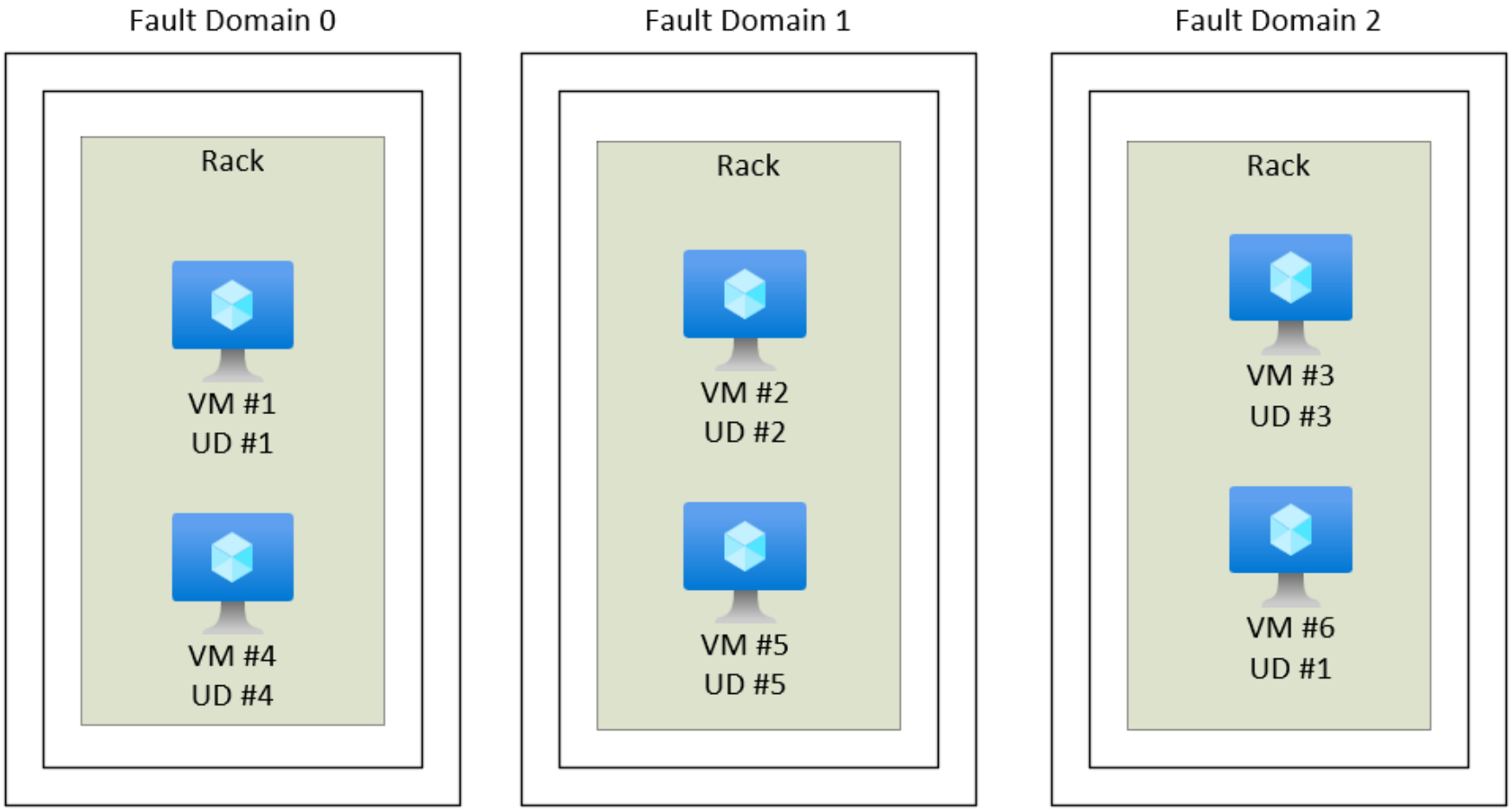
Розміщення в різних зонах: Ви можете розміщувати віртуальні машини з однієї групи доступності в різних зонах доступності одного регіону Azure. Це дозволяє забезпечити стійкість до відмов та високу доступність в разі недоступності однієї зони.

Автоматичне розташування: Azure автоматично розташовує віртуальні машини в групі доступності на різних фізичних серверах і зонах. Ви можете специфікувати, скільки віртуальних машин має бути в групі доступності, і Azure забезпечить їх автоматичне розміщення.

Пов'язані віртуальні машини: Віртуальні машини в групі доступності пов'язані, що означає, що вони спільно користуються мережевими ресурсами та IP-адресами. Це забезпечує збереження стабільності і роботи додатків в разі відмови.

Оновлення і обслуговування: Групи доступності дозволяють проводити обслуговування і оновлення віртуальних машин з мінімальним впливом на доступність вашого додатку.

Групи доступності (Availability Sets)



Azure Defender для віртуальних машин

Виявлення загроз: Azure Defender виявляє загрози та атаки на віртуальні машини, включаючи вразливості, вторгнення, шкідливі програми та інші потенційні загрози.

Моніторинг заходів безпеки: Служба надає можливість моніторити заходи безпеки на віртуальних машинах, а також аналізувати журнали подій для виявлення аномальної активності.

Попередження про загрози в реальному часі: Azure Defender надає попередження про потенційні загрози та вторгнення в реальному часі, дозволяючи оперативно реагувати на ситуації безпеки.

Інтеграція з системами моніторингу і логування: Ви можете інтегрувати Azure Defender з іншими системами моніторингу та логування, щоб отримувати повну картину про безпеку вашого хмарного середовища.

Автоматична реакція на загрози: Azure Defender дозволяє автоматизувати реакцію на загрози, включаючи блокування атак та ізоляцію віртуальних машин для запобігання подальшому поширенню загроз.

Інтеграція з Azure Security Center: Azure Defender для віртуальних машин ідеально поєднується з Azure Security Center, що дозволяє отримати централізоване управління безпекою та аналітику.

Azure Disk Encryption

Шифрування at rest: Azure Disk Encryption забезпечує шифрування даних, збережених на віртуальних жорстких дисках (VHD), пов'язаних з вашими VM, поки вони не використовуються. Це означає, що дані залишаються зашифрованими, коли вони зберігаються на фізичній інфраструктурі Azure.

Інтеграція з Azure Key Vault: Для керування і захисту ключів шифрування Azure Disk Encryption інтегрується з Azure Key Vault. Ключі шифрування, використовувані для шифрування та розшифрування дисків VM, зберігаються безпечно в Azure Key Vault. Це розділення ключів і даних підвищує безпеку.

Підтримувані операційні системи: Azure Disk Encryption підтримує різні операційні системи Windows та Linux, включаючи Windows Server, Ubuntu, CentOS, Red Hat Enterprise Linux (RHEL) і SUSE Linux Enterprise Server (SLES).

Контроль доступу на основі ролей (RBAC): Ви можете контролювати доступ до ключів шифрування, збережених в Azure Key Vault, за допомогою системи RBAC Azure. Це забезпечує, що лише авторизовані користувачі та додатки можуть отримувати доступ до ключів.

Керування дисками: Azure Disk Encryption працює безперешкодно з керованими дисками, що дозволяє вам шифрувати як системні диски, так і дані на дисках для віртуальних машин.

Інтеграція з BitLocker і DM-Crypt: Для віртуальних машин під управлінням Windows, Azure Disk Encryption використовує BitLocker, а для віртуальних машин під управлінням Linux - DM-Crypt. Це стандартні технології шифрування.

Шифрування снапшотів дисків Azure VM: Azure Disk Encryption може також шифрувати снапшоти дисків VM, забезпечуючи захист даних навіть під час створення резервних копій.

Резервне копіювання віртуальних машин в Azure

Azure Backup:

- Azure Backup - це служба резервного копіювання в Azure, яка дозволяє створювати резервні копії ваших віртуальних машин і їх даних. Вона надає можливість налаштовувати регулярне резервне копіювання з можливістю відновлення в будь-який час. Azure Backup також підтримує інкрементальне резервне копіювання, що допомагає зменшити використання мережі та зберігання.

Автоматичне резервне копіювання з використанням Azure Policy:

- Azure Policy дозволяє налаштовувати автоматичне резервне копіювання для ваших віртуальних машин, використовуючи політики Azure. Ви можете визначити, як часто потрібно створювати резервні копії і зберігати їх.

Засоби резервного копіювання сторонніх виробників:

- Поза Azure Backup, ви також можете використовувати сторонні рішення для резервного копіювання, які інтегруються з Azure і надають розширені функції резервного копіювання та відновлення.

Засоби резервного копіювання ОС віртуальної машини:

- Для резервного копіювання операційної системи віртуальної машини (зазвичай C: диск) ви можете використовувати вбудовані засоби операційної системи, такі як Windows Backup або rsync у Linux.

Висновки

- Віртуальні машини Azure - сервіс Microsoft Azure, який надає обчислювальні ресурси без необхідності використання фізичного обладнання
- При виборі віртуальної машини Azure вказується регіон Azure, визначається розмір віртуальної машини та вибирається операційна система віртуальної машини (Windows Server або Linux).
- Для забезпечення обміну даними між багатьма віртуальними машинами Azure та створенню з'єднання з локальною інфраструктурою, використовуються віртуальні мережі.