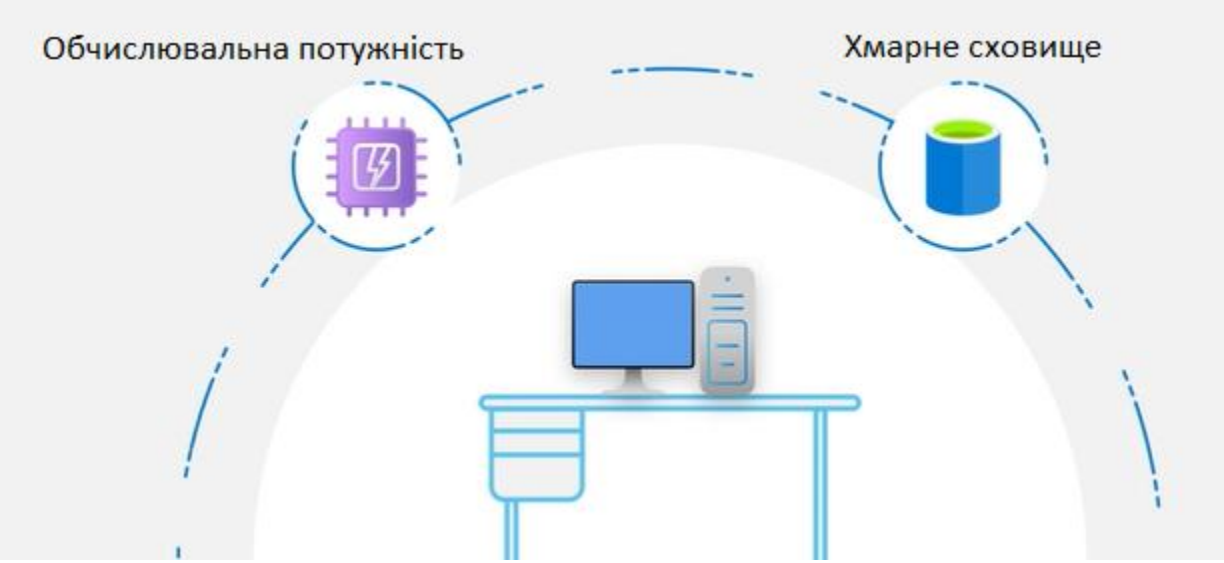
Лекція 1. Основні поняття та класифікація систем хмарних обчислень.

Тема 1. Платформи віртуалізації — платформа Microsoft Azure.

Тема 2. Azure Resource Manager (ARM) — служба розгортання та керування ресурсами платформи Microsoft Azure.

Тема 3. Ресурси платформи Microsoft Azure.

Хмарні технології



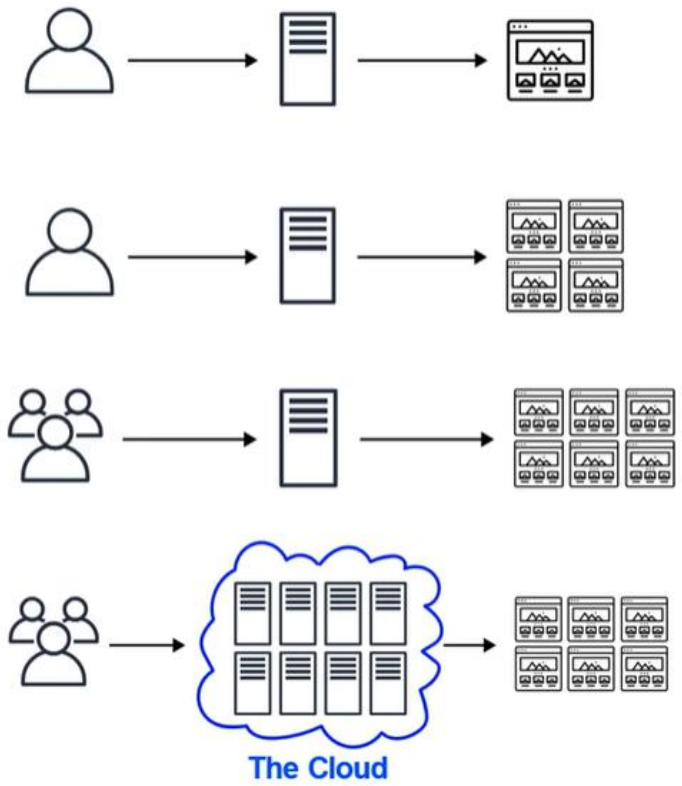
- Хмарне сховище — це модель збереження даних, в якій цифрові дані накопичуються в логічні пули, а фізичне зберігання охоплює кілька серверів.
- Обчислювальна потужність ПК — це кількісна характеристика швидкості виконання певних операцій комп'ютером.

Хмарні технології – це технології в яких комп'ютерні ресурси надаються Інтернет користувачам як онлайн сервіс, за моделлю «хмарних обчислень».

«*Хмарні обчислення*» - це модель надання обчислювальних послуг через Інтернет. Обчислювальні послуги включають загальну IT-інфраструктуру, таку як віртуальні машини, сховище, бази даних і мережу. Хмарні сервіси також розширюють традиційні IT-пропозиції, включаючи такі речі, як Інтернет речей (IoT), машинне навчання (ML) і штучний інтелект (AI).

Головна відмінність полягає в тому, що ваші комп'ютерні ресурси знаходяться у компанії, яка надає «хмарні» послуги. Всі провайдери «хмарних обчислень» надають ресурси такі як «Хмарне сховище», «Обчислювальні потужності».

Особлтвість – ви завжди можете замовите більший об'єм сховища і більшу обчислювану потужність і вам для цього не потрібно купувати новий ПК.



Розвиток обчислювальних потужностей

- Локальний сервер - Всі організації мають Се́рвер у локальній мережі, який надає користувачам свої обчислювальні і дискові ресурси, а також доступ до встановлених сервісів; найчастіше працює цілодобово, чи у час роботи групи його користувачів.

Проблеми: великі фінансові витрати, потужності сервера швидко починає не вистачати.

- Віртуальний виділений-приватний сервер (англ. virtual dedicated server),— послуга, в рамках якої користувачеві надають віртуальний сервер. Це повноцінна альтернатива фізичного виділеного сервера з великою кількістю переваг, високою стабільністю, простотою в управлінні і налаштуванні, стійкістю до відмов і набагато меншими фінансовими витратами.
- Віртуальний публічний сервер – дуже не дорогий, але може не вистачити ресурсів для всі клієнтів, у випадках, коли хтось вимагає багато ресурсів.
- «Хмара» - інфраструктура обчислювальних служб, які надаються відповідно до запиту.

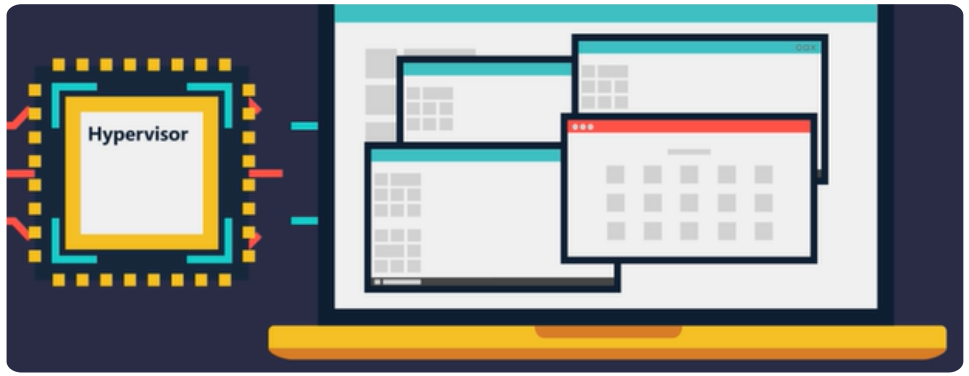
Десяткова система			
Назва	**Скорочення**		**Степінь**
байт	Б	(B)	10^{0}
кілобайт	кБ	(кВ)	10^{3}
мегабайт	МБ	(МВ)	10^{6}
гігабайт	ГБ	(GB)	10^{9}
терабайт	ТБ	(ТВ)	10^{12}
петабайт	ПБ	(РВ)	10^{15}
ексабайт	ЕБ	(ЕВ)	10^{18}
зетабайт	ЗБ	(ZB)	10^{21}
йотабайт	ЙБ	(YB)	10^{24}

Чому виникла потреба у «хмарі»? - Зростання обсягів даних, у тому числі.

- За прогнозами, в 2025 році обсяг даних буде сягати 175,8 зетабайт. Для порівняння, в 2015 році даних було в розмірі 18,2 зетабайт.
- За прогнозами, до 2025 року обсяг даних у сховищах зросте з 0,8 зетабайт до 9 зетабайт.
- За прогнозами, до 2025 року обсяг пам’яті пристроїв для зберігання даних, таких як оптичних дисків, стрічкових і твердих накопичувачів, збільшитися до 12,6 зетабайт у компаніях. У хмарні сховища будуть відправляти 50% від цього обсягу.
- Уже до 2025 року компанії будуть зберігати 80% даних на периферії і в центрі. У 2015 році компанії розміщали тільки 35% даних в такі сховища.

Популярні сфери використання хмарних обчислень

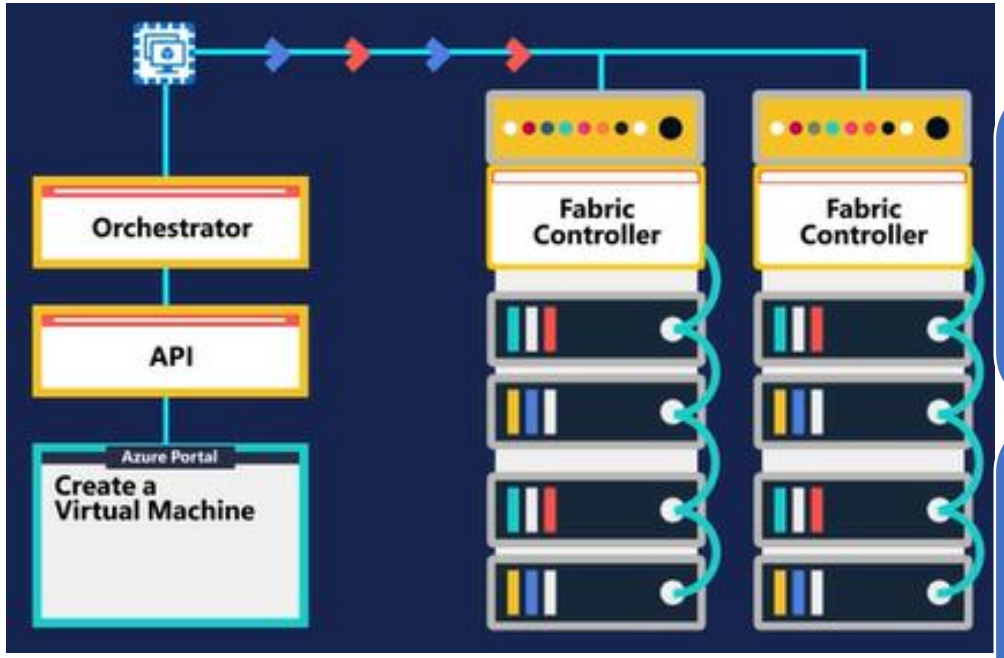
- ❖ Управління бізнесом - хмарні рішення, такі як корпоративні портали, віддалені робочі столи, системи для управління ресурсами клієнтів і планування ресурсів компанії. Приклади: Marketo, Salesforce, Hubspot, Dynamics 365.
- Освіта - 70-80% навчальних закладів у всьому світі вже впровадили хмарні обчислення в освітніх цілях. На LMS (Learning Management System) поміщають весь освітній контент, яким обмінюються викладачі та студенти. Корпорації - створюють власні освітні платформи, де кожен може отримати доступ до матеріалів за певну оплату, приклад – Amazon Web Service.
- ❖ Охорона здоров'я –медичні установи створюють електронні медичні записи в хмарі. Публічні хмари Microsoft Azure, IBM Cloud, хмара від Dell, або ж приватна хмара – приклади платформ хмарних обчислень для сфери охорони здоров'я
- ❖ Стрімінгові розважальні платформи – Netflix, Amazon, YouTube та інші – їх потокові сервіси мігровані в «хмару».



Віртуалізація – поняття

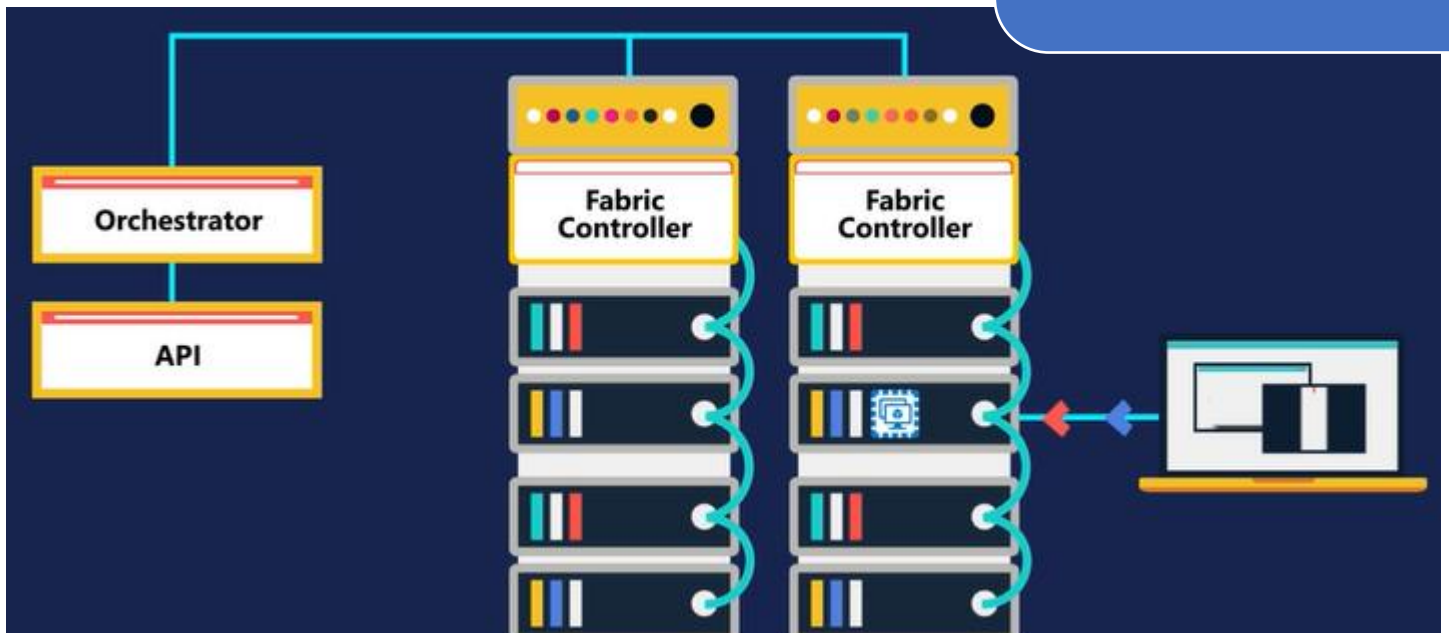
- Поняття «хмара» тісно пов'язане з поняттям *віртуалізація*, тобто створенням віртуального об'єкта чи середовища. Віртуалізація забезпечує можливість використання не реальні ресурсів а їх програмного емулятора, який у свою чергу використовує частину фізичного ресурсу - серевера.
- Віртуалізація — це технологія, яка дозволяє кільком віртуальним машинам (ВМ) або віртуальним середовищам працювати на одній фізичній машині (сервері), спільним використанням її ресурсів, залишаючись ізольованим одна від одної.
- ОС відділяться від ЦП шаром, який називається Гіпервізор, і який забезпечує виконання багатьох ВМ з різними ОС-ми на одному сервері.

Віртуалізація - поняття



Сервери, кожен із своїм гіпервізором, розташовуються в будівлі, яка називається – центром обробки даних (datacenter). Сервери поміщаються у шафи, які з'єднані мережевим комунікатором для забезпечення підключення до мережі та розподілу живлення. Шафи обладнані - контролером структури (Fabric Controller) – це програма, яка забезпечує роботу серверів. Контролери об'єднані під управлінням програми – зовнішнього інтерфейсу (Orchestrator).

Коли від користувача приходить запит на створення ресурсу, то зовнішній інтерфейс спочатку перевіряє, чи має користувач на це ліцензію, і якщо так, то направляє його до серверу, де і створюється ресурс.



Типи віртуалізація.

- Віртуалізація платформи - відокремлює операційну систему від ресурсів платформи.
- Віртуалізація прикладного програмного забезпечення, виконання окремих програм на відмінній апаратній/програмній платформі.
- Крос-платформова віртуалізація, дозволяє програмному забезпеченню скомпільованому для певного процесору та операційної системи працювати на відмінних процесорах та/або операційних системах.
- Віртуальний пристрій, образ віртуальної машини призначений для роботи на віртуалізованій платформі.
- Віртуалізація сховища, процес повного абстрагування логічного сховища даних від фізичного сховища.
- Мережева віртуалізація, створення віртуалізованого адресного простору мережі в середині або через існуючі підмережі.
- Віртуальна приватна мережа (VPN), комп'ютерна мережа, в які деякі канали зв'язку між вузлами створені через відкриті канали передачі даних або віртуальні канали у більших мережах, таких як Інтернет

Які проблеми вирішує віртуалізація?

Ефективне використання ресурсів: Віртуалізація дозволяє консолідувати сервери та максимально ефективно використовувати вільні ресурси, знижуючи при цьому витрати на обладнання та енергію.

Швидке розгортання нових середовищ: Віртуалізація дозволяє швидко створювати і налаштовувати нові віртуальні машини для розгортання нових програм та сервісів.

Гнучкість управління: Завдяки віртуалізації легше управляти і масштабувати інфраструктуру, адаптуватись до змін навантаження та потреби бізнесу.

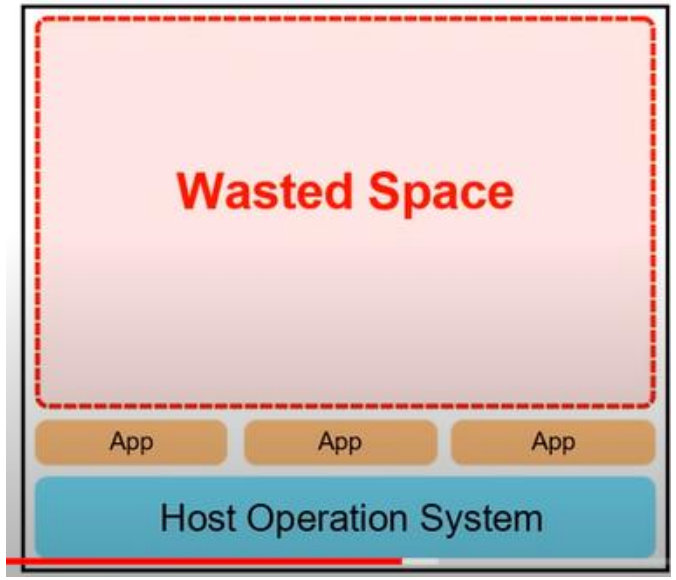
Запобігання втратам даних: Віртуалізація сприяє більш ефективному резервному копіюванню та відновленню даних, а також міграції даних між серверами без перерви у роботі.

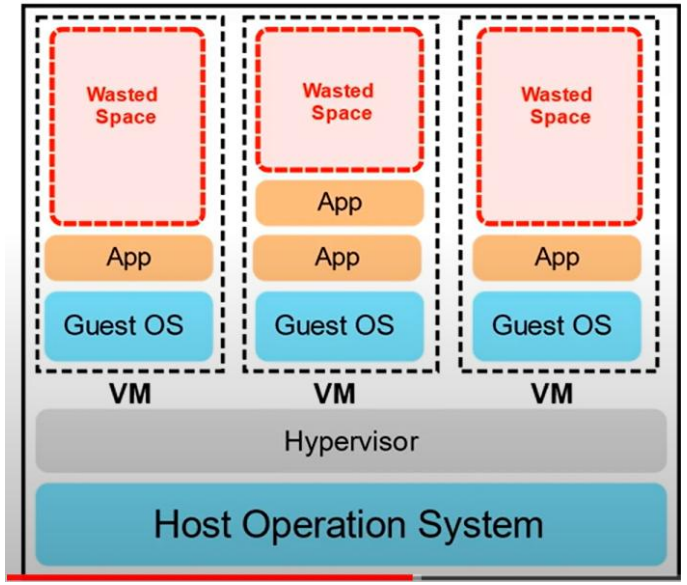
Підвищена безпека: За допомогою віртуалізації можна впроваджувати більш строгі політики безпеки і ізоляції між віртуальними машинами, що покращує загальну безпеку систем.

Зменшення впливу відмови обладнання: Віртуалізація дозволяє швидко переміщати віртуальні машини між фізичними серверами у випадку відмови обладнання, знижуючи час простою.

Спрощення тестування та розробки: Віртуалізація надає ізольовані середовища для розробки та тестування, що дозволяє розробникам експериментувати без ризику для виробничих систем.

Ключові компоненти віртуалізації





Гіпервізор: Це програмне забезпечення, яке створює та керує віртуальними машинами (ВМ) на фізичному сервері. Гіпервізор може бути типу 1 (bare-metal), який працює безпосередньо на обладнанні, або типу 2 (хостований), який працює на операційній системі хоста.

Віртуальні машини (VM): Віртуальні машини є емульованими комп'ютерами, які працюють всередині фізичного сервера і мають свою власну операційну систему та програми, але ділять фізичні ресурси з іншими ВМ.

Віртуальний менеджер ресурсів: Цей компонент керує розподілом ресурсів між віртуальними машинами, включаючи ЦП, пам'ять, мережу і зберігання даних.

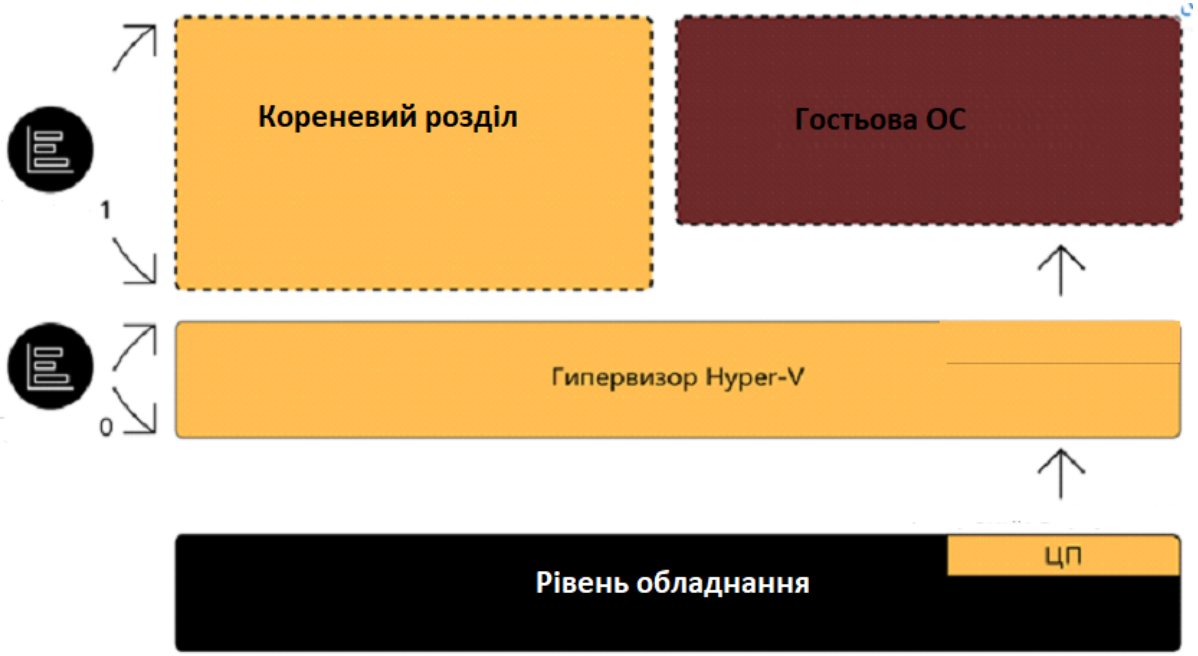
Віртуальна мережа: Віртуальна мережа дозволяє віртуальним машинам взаємодіяти одна з одною і з зовнішніми мережами, імітуючи роботу фізичної мережі.

Віртуальне зберігання: Подібно до віртуальної мережі, віртуальне зберігання використовує програмне забезпечення для створення ілюзії фізичних пристроїв зберігання даних для ВМ.

Консоль управління: Це інтерфейс адміністратора, який дозволяє моніторувати, керувати і конфігурувати віртуальні середовища, ВМ, мережі та зберігання.

Консолідована інфраструктура: Програми і обладнання, які дозволяють гнучко і ефективно розгортати віртуальні середовища, включаючи рішення для резервного копіювання, моніторингу і безпеки.

Hyper-V - технологія віртуалізації, розроблена Microsoft.



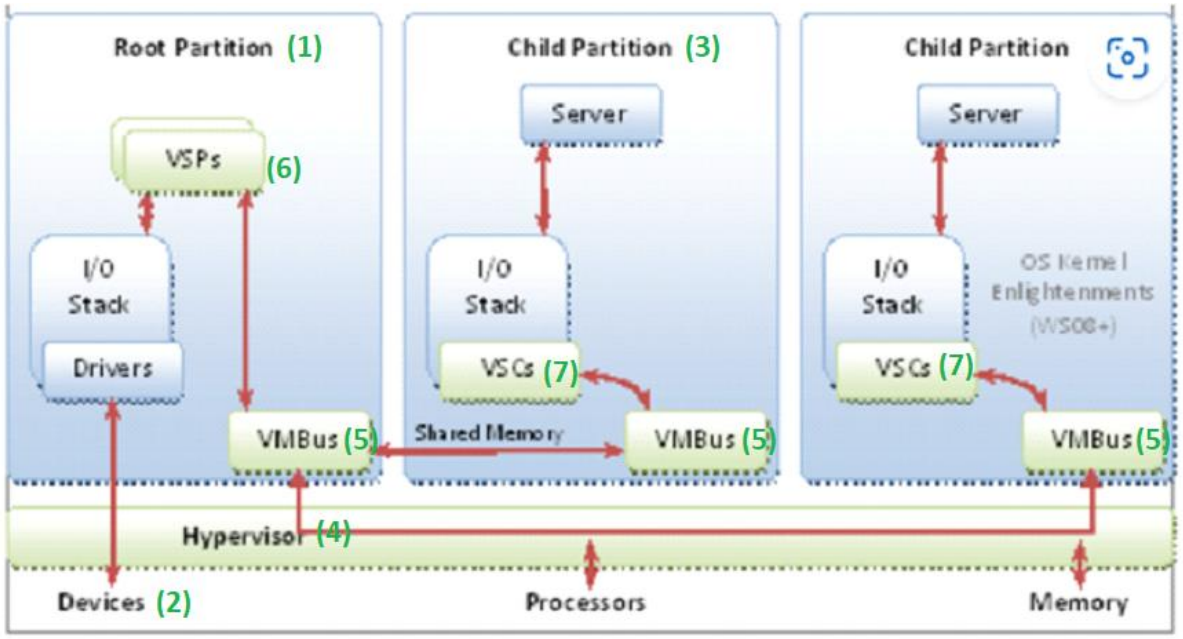
Архітектура Hyper-V складається з 3х рівнів:

рівень - 0 – рівень обладнання;

рівень - 1 – гіпервізор Hyper-V;

рівень - 2 – кореневий розділ та гостьова ОС

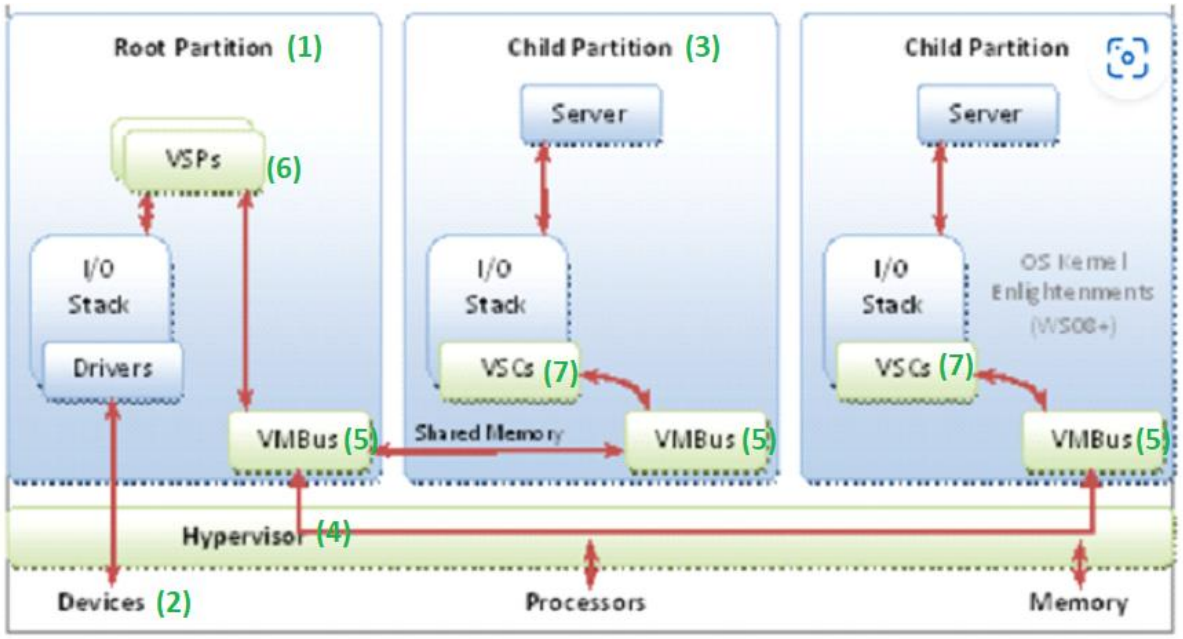
Hyper-V - архітектура



Кореневий розділ (1), апаратні пристрої (2), дочірні розділи (3), Гіпервізор (4), канал яким здійснюється взаємодія між розділами (5), постачальники служб віртуалізації (6), клієнти служб віртуалізації (VSC) (7)

- Hyper-V повинен мати один кореневий розділ під керуванням Windows.
- Кореневий розділ - створюється першим і має всі ресурси, не пов'язані з гіпервізором, включаючи більшість пристроїв і системної пам'яті. У кореневому розділі розміщується стек віртуалізації, а також створюються та керуються дочірні секції.
- Стек віртуалізації - колекція програмних компонентів у кореневому розділі, які працюють разом для підтримки віртуальних машин. Стек віртуалізації запускається у кореневому розділі (1) і має прямий доступ до апаратних пристроїв (2).
- Кореневий розділ породжує дочірні розділи (3), у яких розташовуються гостьові ОС. Кореневий розділ створює дочірні за допомогою API-інтерфейсу гіпердзвінка.

Hyper-V - дочірні розділи



Кореневий розділ (1), апаратні пристрої (2), дочірні розділи (3), Гіпервізор (4), канал яким здійснюється взаємодія між розділами (5), постачальники служб віртуалізації (6), клієнти служб віртуалізації (VSC) (7)

У дочірніх розділах немає доступу до фізичного процесора і вони не обробляють переривання процесора. Дочірні розділи також не мають прямого доступу до інших апаратних ресурсів.

Дочірні розділи роблять запити доступу до ресурсів, які приймають клієнти служб віртуалізації (VSC) та перенаправляють до каналу VMBus.

Постачальники служб віртуалізації (VSP) в кореневому розділі підключаються до шини VMBus та обробляють запити на доступ до пристроїв від дочірніх розділів.

Низькорівнева оболонка Hyper-V повністю контролює можливості апаратної віртуалізації та не надає їх гостьовій операційній системі (гостяній ОС).

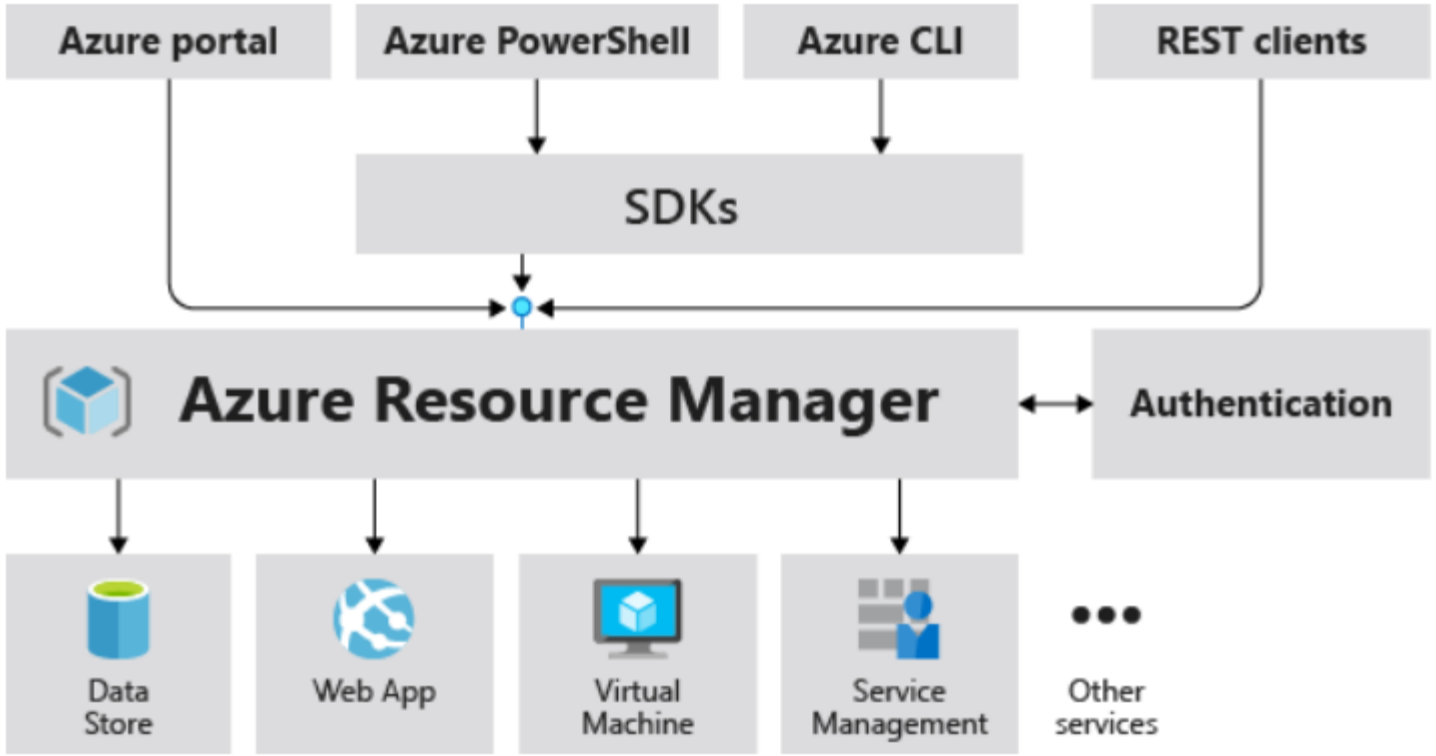
Платформи віртуалізації.

- Hyper-V — це платформа віртуалізації, надана Microsoft для операційних систем Windows Server і Windows. Це дозволяє користувачам створювати віртуальні машини та керувати ними на хост-машині Windows.
- VMware vSphere — це платформа віртуалізації та хмарних обчислень, розроблена компанією VMware, Inc. Вона надає набір інструментів і технологій для створення віртуалізованих середовищ центрів обробки даних і керування ними. VMware vSphere включає ESXi гіпервізор. Він забезпечує основні функції віртуалізації, безпосередньо керуючи апаратним забезпеченням сервера та дозволяючи створювати та запускати віртуальні машини.
- Citrix - багатонаціональна компанія з програмного забезпечення, яка надає ряд продуктів і рішень, пов'язаних із віртуалізацією, хмарними обчисленнями та мережами. Основна увага Citrix зосереджена на наданні віддаленого доступу, інфраструктури віртуального робочого столу (VDI) і рішень для доставки додатків для підприємств і організацій.
- Microsoft Azure часто згадується просто як Azure — хмарна платформа та інфраструктура корпорації Microsoft, призначена для розробників застосунків хмарних обчислень (англ. cloud computing) і покликана спростити процес створення онлайнових додатків. Microsoft Azure дозволяє розгортати додатки як за допомогою Microsoft .NET і Visual Studio, так і за допомогою інших інструментів. Платформа працює на серверах Microsoft.

Платформа Microsoft Azure- https://portal.azure.com

Платформа Microsoft Azure- https://portal.azure.com

Azure Resource Manager (ARM) — це служба розгортання та керування для Azure. Яка дає змогу створювати, оновлювати та видаляти ресурси у вашому обліковому записі Azure.



ARM дозволяє групувати пов'язані ресурси в контейнери, відомі як ресурсні групи.

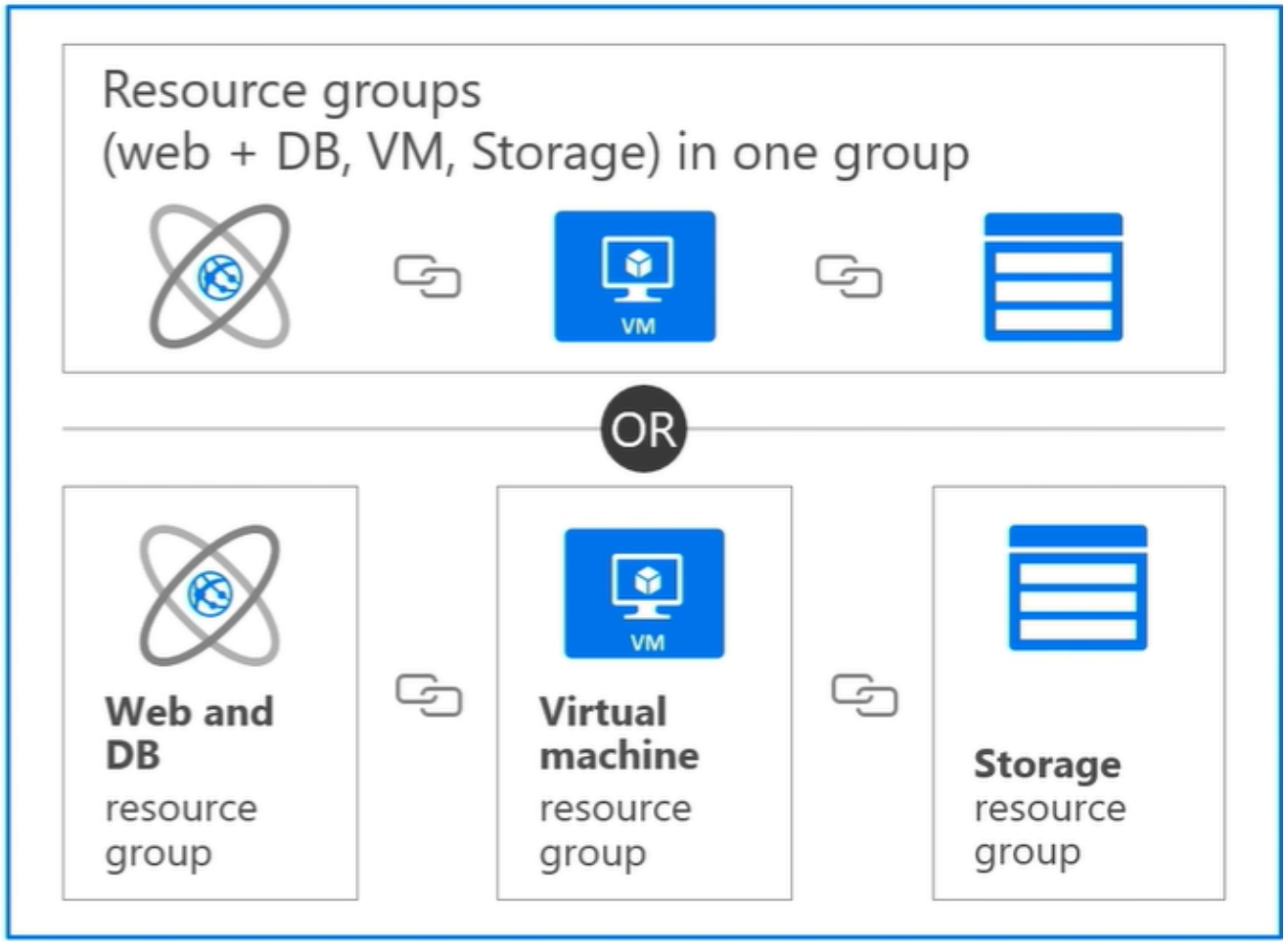
ARM інтегрується з Azure Active Directory і підтримує модель контролю доступу на основі ролей (RBAC), дозволяючи деталізовано управляти доступом до ресурсів.

ARM надає інструменти для управління життєвим циклом ресурсів, включаючи оновлення, масштабування та видалення ресурсів.

Усі можливості, доступні на порталі, також доступні через PowerShell, Azure CLI, REST API та клієнтські SDK.

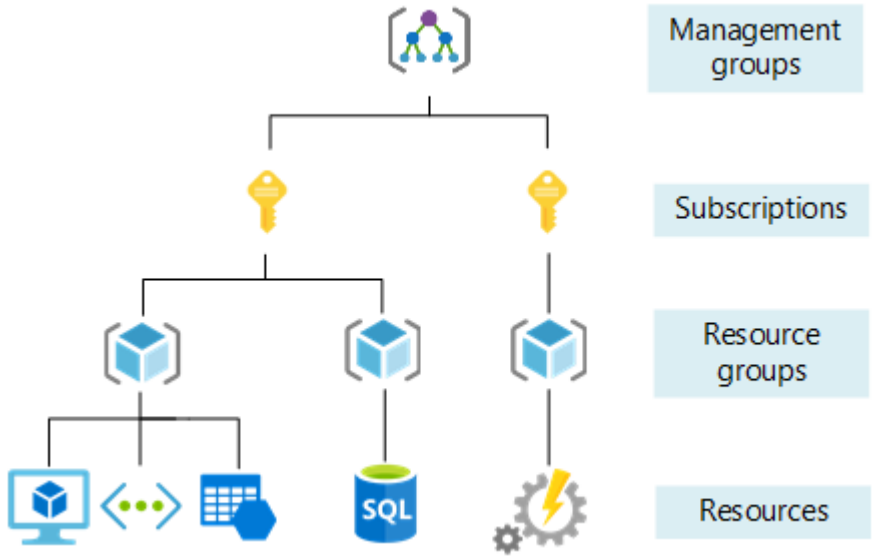
Azure Resource Manager - Терміни

1. Ресурс – керований елемент, доступний через Azure. Прикладами ресурсів є віртуальні машини, облікові записи зберігання, веб-програми, бази даних і віртуальні мережі.
2. ***Група ресурсів*** – контейнер, який містить пов'язані ресурси. Група ресурсів включає ті ресурси, якими ви хочете керувати як групою. Групи ресурсів не можуть бути вкладені одна в одну.
3. ***Постачальник ресурсів*** – служба, яка надає ресурси Azure. Наприклад, поширеним постачальником ресурсів є Microsoft.Compute, який надає ресурс віртуальної машини.
4. Шаблон ARM – файл нотації об'єктів JavaScript (JSON), який визначає один або кілька ресурсів для розгортання. Шаблон можна використовувати для послідовного та багаторазового розгортання ресурсів.
5. Ресурс розширення – ресурс, який додає можливості іншого ресурсу. Наприклад, призначення ролі є додатковим ресурсом.



Рівні управління

Azure надає чотири рівні управління: групи керування (management groups), підписки (subscriptions), групи ресурсів (resource groups) і ресурси (resources).



Групи керування (Management groups) – необхідні для ефективного керування доступом, політиками та відповідністю для цих підписок. Групи керування забезпечують область управління над підписками (subscriptions). Умови керування, які ви застосовуєте, успадковуються каскадом до всіх пов’язаних підписок.

Підписки (subscriptions) в основному є домовленістю з Microsoft про використання одного або декількох їх хмарних сервісів. Ключові цілі підписки Azure:

Управління ресурсами: Підписка Azure служить одиницею виставлення рахунків і допомагає управляти ресурсами, створеними користувачами. Користувачі можуть групувати та управляти пов'язаними ресурсами разом, пов'язавши їх з тією самою підпискою.

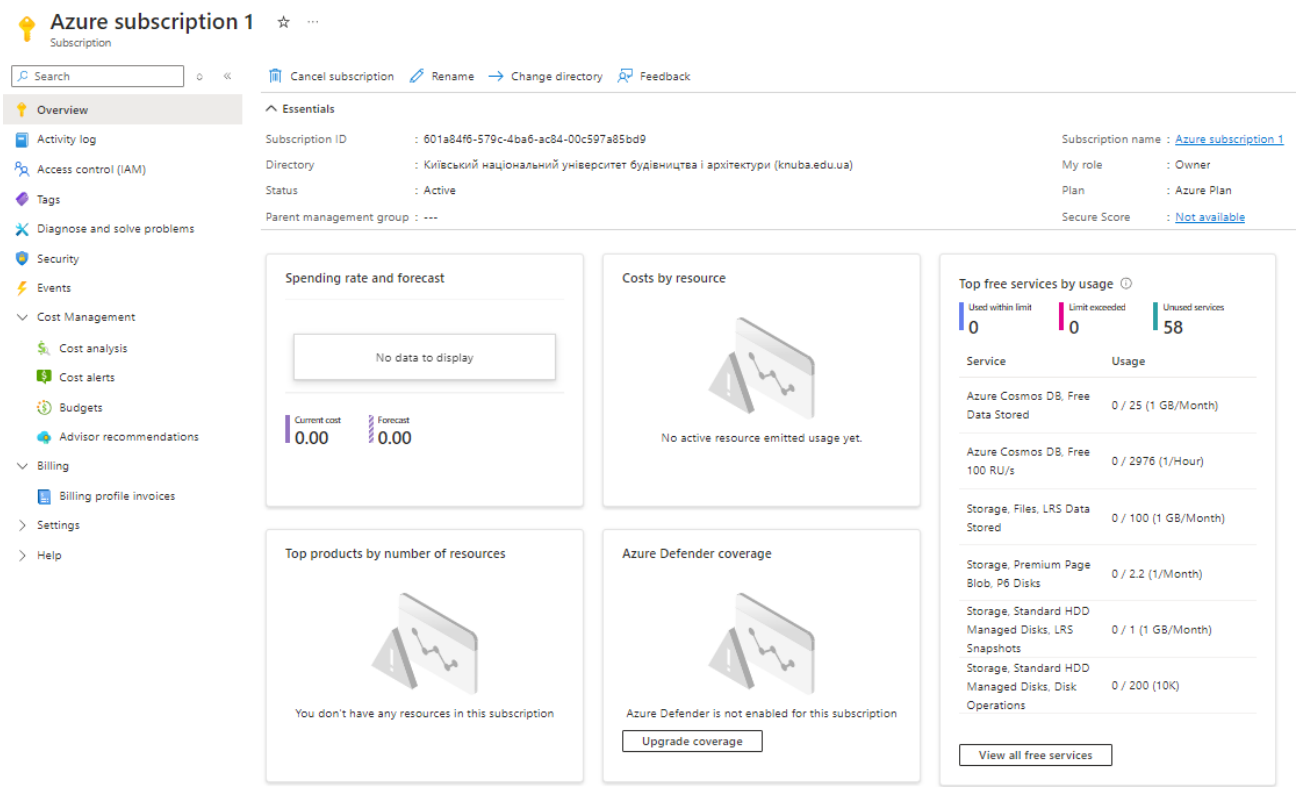
Управління доступом: Підписка також надає засоби адміністраторам для надання дозволів на доступ до облікових записів користувачів, груп та додатків для управління ресурсами в межах підписки.

Відстеження вартості та виставлення рахунків: Кожне використання сервісу входить до конкретної підписки, і це сприяє контролю за витратами, використанням ресурсів та лімітами витрат.

Створення ізоляції: Різні підписки можуть використовуватися для створення логічної ізоляції ресурсів та застосування політик управління в межах організації.

Використання сервісів: З підпискою ви погоджуєтесь на деякі умови та положення щодо використання сервісів Azure. Сервіси Azure доступні тільки тоді, коли у вас активна підписка.

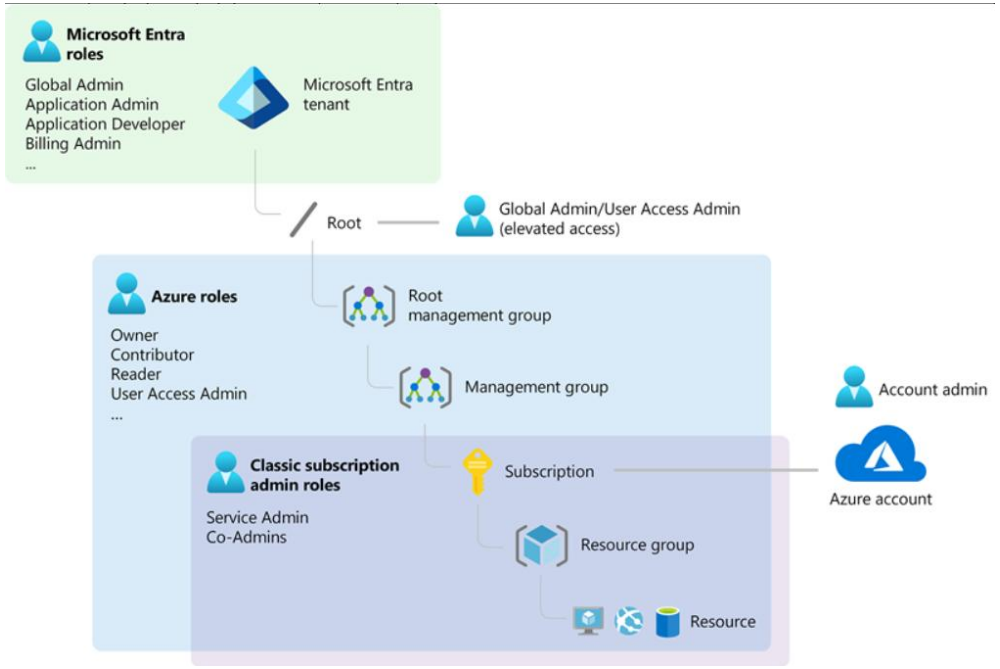
Основні параметри підписки



1. Керування доступом (IAM) – це сторінка, для призначення ***ролей*** для надання доступу до ресурсів Azure.
2. Azure теги (Tags) — це елементи метаданих (у форматі ключ-значення), які допомагають організувати та відслідковувати ресурси.
3. Безпека (Security).
4. Управління витратами (Cost Analysis).
5. Рахунки (Billing profiles).
6. Функція "Діагностика та усунення проблем”.
7. Опція «Налаштування» (Settings).

Керування доступом (IAM) до ресурсів за допомогою Azure RBAC полягає в призначенні ролей Azure, які слід розуміти – як спосіб застосування дозволів. Azure RBAC — це система авторизації, створена на базі диспетчера ресурсів Azure, яка забезпечує точне керування доступом до ресурсів Azure. Azure RBAC містить понад **100 вбудованих ролей**. Існує п’ять основних ролей Azure. Перші три застосовуються до всіх типів ресурсів:

1. «Власник» (Owner) - Надає повний доступ до керування всіма ресурсами. Призначає ролі в Azure RBAC. Роль належить Адміністратору служби Azure.
2. “Спів-власник” (Contributor)- Надає доступ до керування ресурсами включеними в групи керування.
3. «Читач» (Reader) - має доступ до ресурсів без права внесення змін.

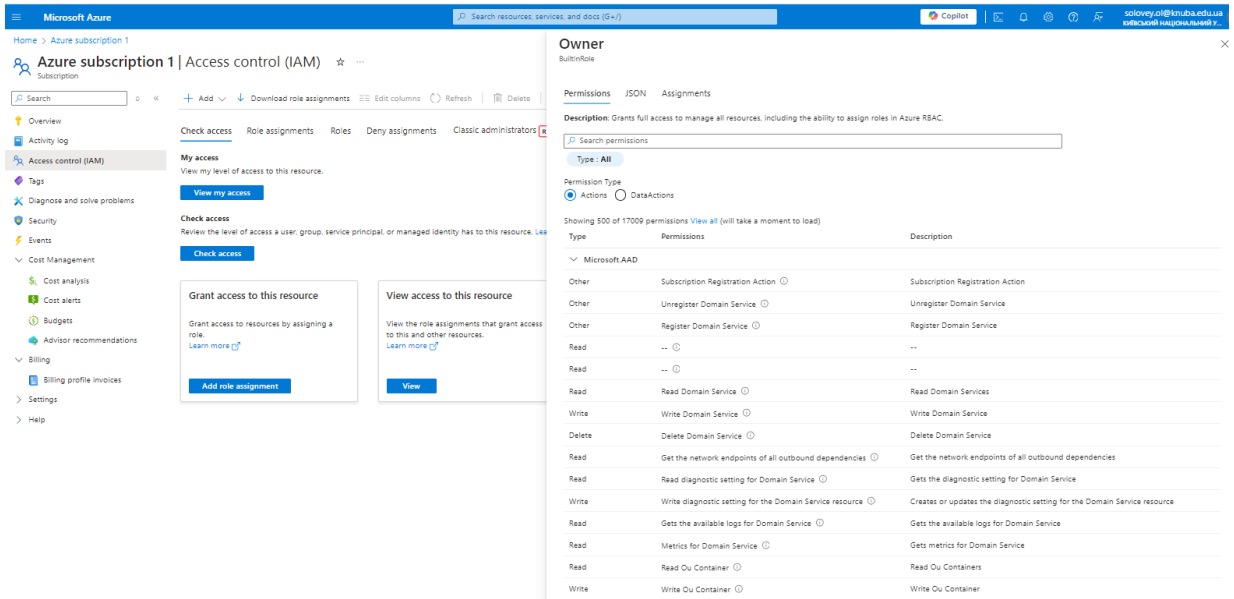


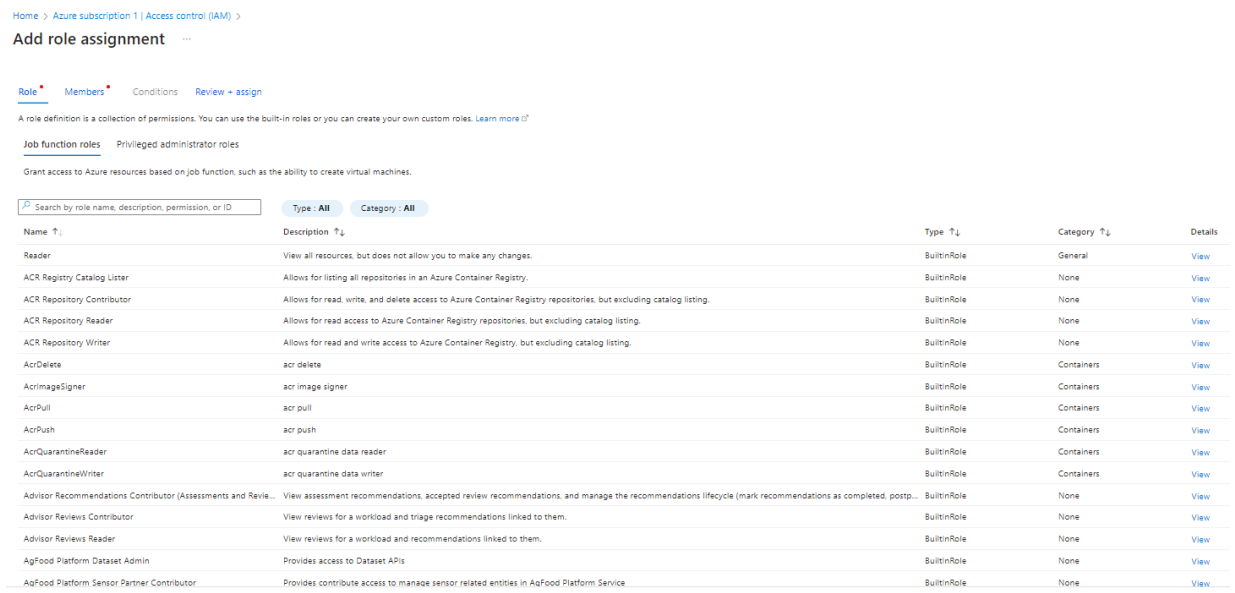
Microsoft Entra ID — це хмарна служба керування ідентифікацією та надання доступу до зовнішніх ресурсів. Приклади ресурсів включають Microsoft 365, портал Azure та тисячі інших програм SaaS.

IT-адміністратори використовують Microsoft Entra ID для контролю доступу до програм і ресурсів програм відповідно до бізнес-вимог. Наприклад, як IT-адміністратор ви можете використовувати Microsoft Entra ID, щоб вимагати багатофакторну автентифікацію.

Розробники програм можуть використовувати Microsoft Entra ID, для створення персоналізованого досвіду з використанням організаційних даних або додати систему єдиного входу (SSO) до програм.

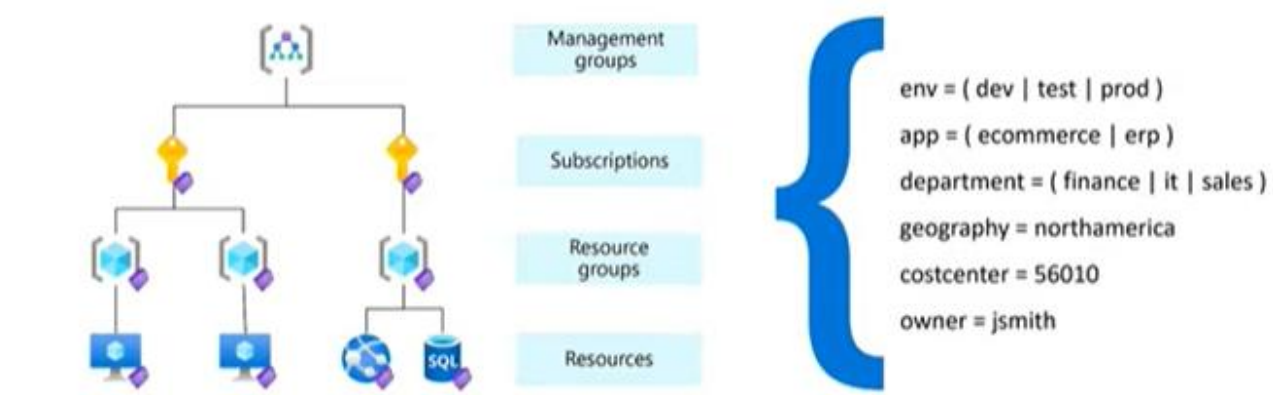
Для підписок, які створені вами – ви є «Власник». Для визначення інших ролей Вам потрібно меню «**Add role assignment**».





Azure Тегі (TAGs) — це елементи метаданих (у форматі ключ-значення), які допомагають організувати ресурси. Загальні типи тегів включають:

1. Environment (Середовище): Вказують на середовище розгортання, таке як Production, Development, Testing (Тестування).
2. Department (Відділ): Ідентифікують відділ, відповідальний за ресурс.
3. Cost Center (Центр витрат): Пов'язують ресурси з конкретними фінансовими рахунками.
4. Project: Вказують на проєкт, який підтримують ресурси.
5. Owner (Власник): Ідентифікують особу або команду, відповідальну за ресурс.
6. Location (Місцезнаходження): Вказують на географічне місцезнаходження ресурсу.
7. Application (Застосунок): Пов'язують ресурси з певними застосунками.



Розглянемо приклад, коли в межах підписки необхідно відслідкувати ресурси за регіоном «East US». Спочатку створимо тег: Location = East US

Нехай маємо дві групи в різних регіонах: «East US» ; “West US”

Create a resource group ...

Validation passed.

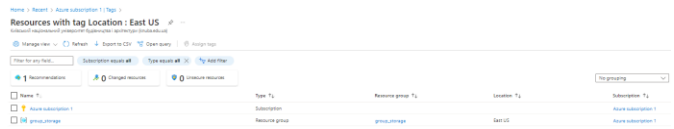
Basics Tags Review + create

Basics

Subscription	Azure subscription 1
Resource group	group_storage
Region	East US

Tags

Location	East US



Create a resource group ...

Validation passed.

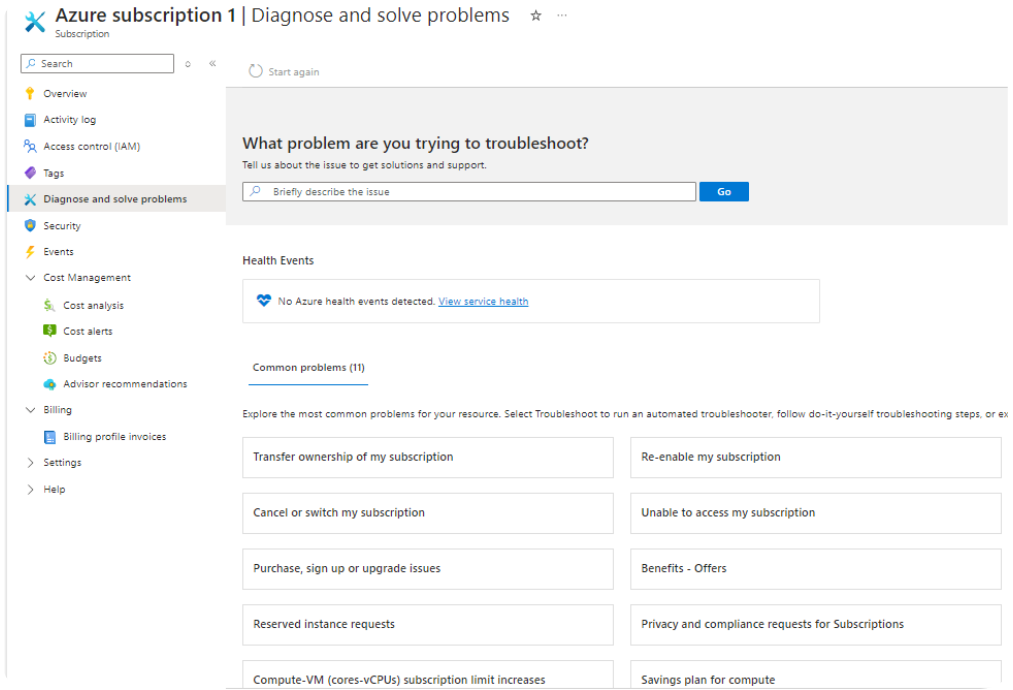
Basics Tags Review + create

Basics

Subscription	Azure subscription 1
Resource group	group_data
Region	West US

Tags

Location	East US



- Опція "Діагностування та вирішення проблем" у підписці Azure надає кілька функцій, спрямованих на допомогу користувачам у виправленні та ефективному вирішенні проблем:
- ***Моніторинг та аналітика***: Надаються інструменти та ресурси для моніторингу стану та продуктивності послуг та ресурсів Azure. Це включає доступ до метрик, журналів та діагностичних даних, які допомагають в ідентифікації та діагностиці проблем.
- ***Рекомендації Azure Advisor***: Azure Advisor надає персоналізовані рекомендації на основі найкращих практик використання Azure для оптимізації ресурсів, підвищення безпеки та покращення продуктивності.
- ***Стан ресурсів***: Надається можливість отримати інформацію про поточний стан ресурсів Azure, що дозволяє швидко виявляти наявні проблеми або перебої, які впливають на ваші ресурси.
- ***Стан послуг***: Надаються відомості про загальний стан та доступність послуг та регіонів Azure, включаючи поточні інциденти та заплановані технічні роботи, які можуть впливати на ваші послуги.

Управління витратами (Cost Analysis)

Моніторинг і звітність: Надає інструменти для моніторингу та аналізу витрат на послуги Azure. Це включає деталізовані звіти і панелі приладів, які надають інформацію про споживання ресурсів і витрати.

Бюджетування: Користувачі можуть встановлювати бюджети для відстеження витрат за конкретними фінансовими межами. ***Можливе налаштування сповіщень*** для повідомлення зацікавлених сторін про наближення або перевищення встановлених лімітів.

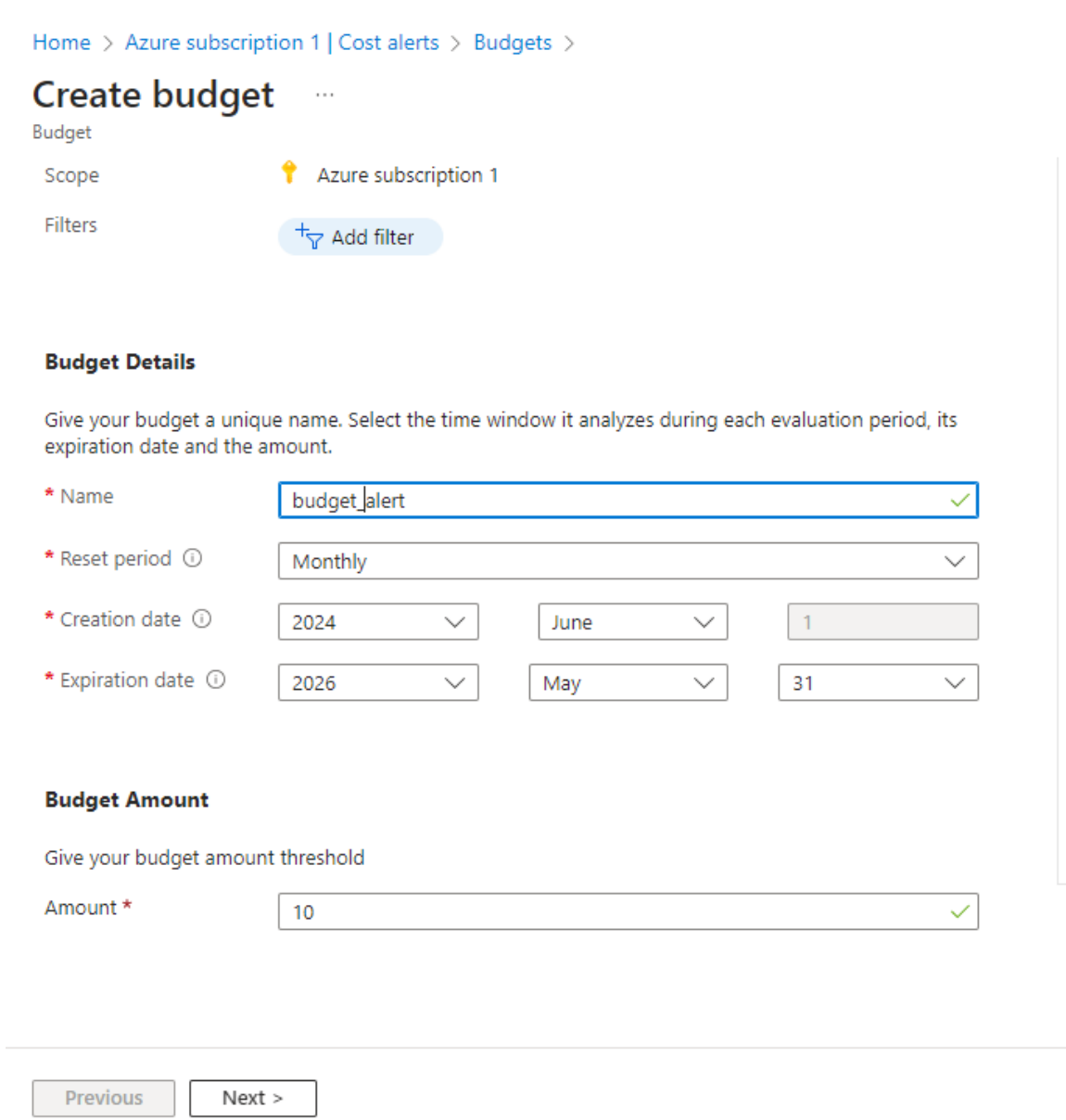
Прогнозування: Допомагає в прогнозуванні майбутніх витрат на основі історичних даних та тенденцій, що дозволяє організаціям ефективно планувати та розподіляти ресурси.

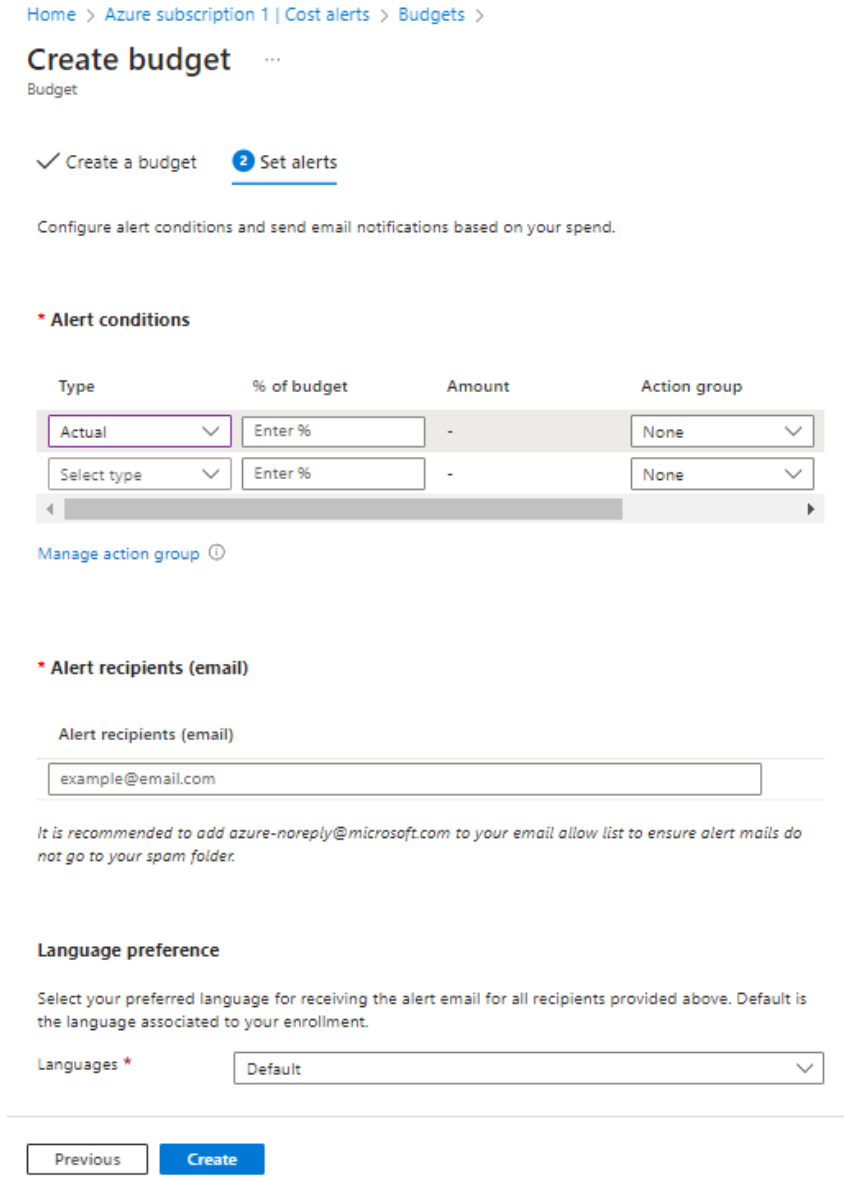
Розподіл витрат: Дозволяє встановлювати мітки і категоризувати ресурси для точного обліку витрат за відділами, проектами або центрами витрат.

Рекомендації: Надає рекомендації з економії коштів на основі використання і найкращих практик Azure. Ці рекомендації допомагають оптимізувати витрати, ідентифікуючи недоексплуатовані ресурси або рекомендуючи придбати зарезервовані екземпляри, де це можливо.

Інтеграція: Інтегрується з Azure Advisor та іншими сервісами Azure для надання комплексних рекомендацій з управління витратами, безпекою, продуктивністю та ефективністю операцій.

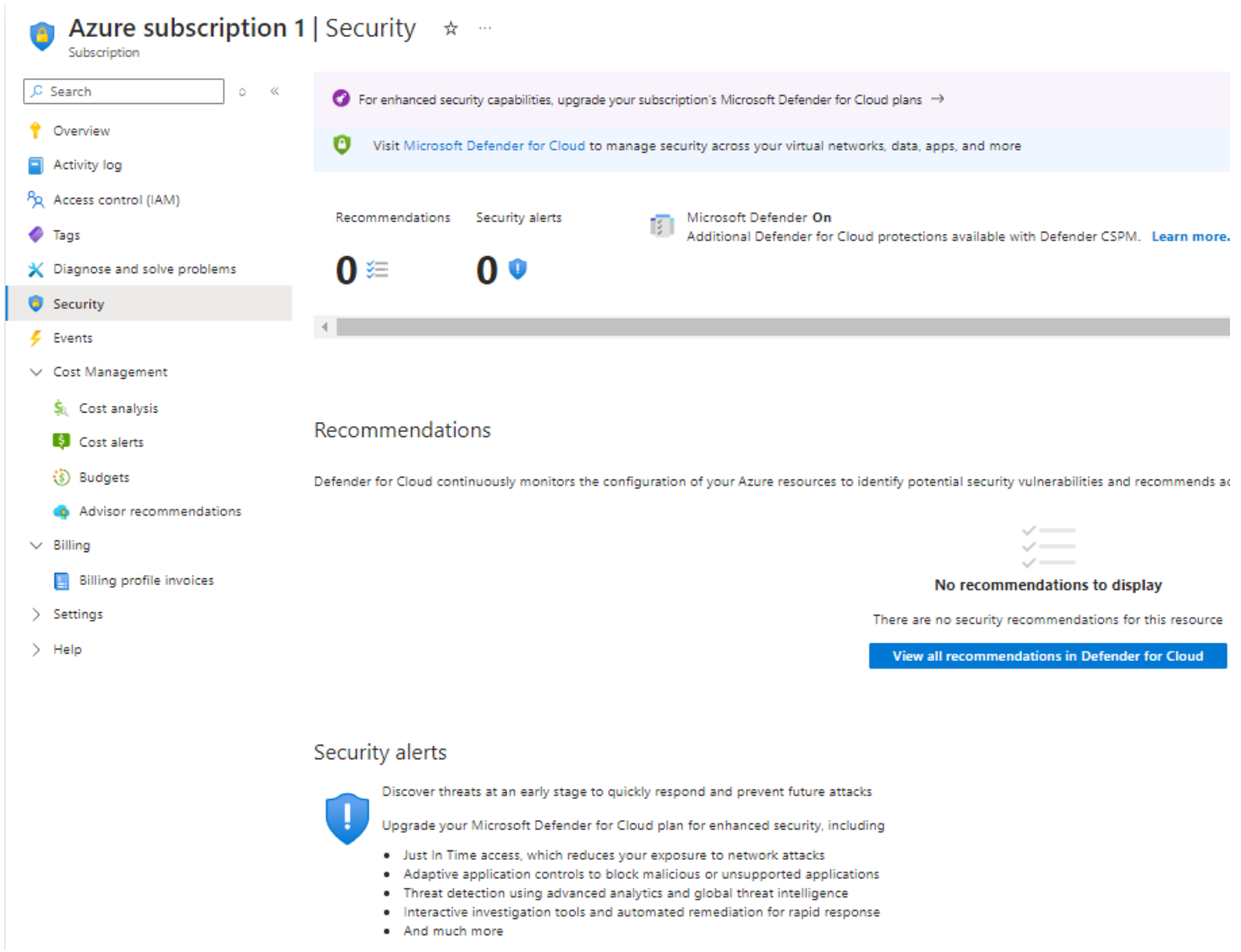
Приклад - ***налаштування сповіщень*** для повідомлення про наближення або перевищення встановлених лімітів





Опція "Безпека"

- Захист від загроз: Виявлення та зменшення потенційних загроз безпеці.
- Управління відповідністю: Забезпечення відповідності ресурсів стандартам та регуляторним вимогам у сфері безпеки.
- Стан безпеки: Надання огляду конфігурацій безпеки та рекомендацій.
- Оцінка вразливостей: Виявлення вразливостей в ваших ресурсах.
- Контроль доступу: Управління дозволами та доступом до ресурсів.



Групу ресурсів можна використовувати для керування доступом визначивши політики Azure.

Assign policy

Basics | Advanced | Parameters | Remediation | Non-compliance messages | Review + create

Scope

Scope Learn more about setting the scope *

Azure subscription 1

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition *

Assignment name *

Description

Policy enforcement

Enabled | Disabled

Assigned by

Ольга Соловей

Review + create | Cancel | Previous | Next

Available Definitions

Search

Type : 2 selected

- Select all
- Custom
- Built-in

POLICY NAME		TYPE
Audit virtual machines without disaster recovery configured		BuiltIn
Vulnerability assessment should be enabled on your Synapse workspaces	Synapse	BuiltIn
Enable logging by category group for microsoft.networkcloud/storageappliances t...	Monitoring	BuiltIn
SQL Server Integration Services integration runtimes on Azure Data Factory should ...	Data Factory	BuiltIn
[Preview]: Configure VMSS created with Shared Image Gallery images to install the ...	Security Center	BuiltIn
Private endpoint connections on Batch accounts should be enabled	Batch	BuiltIn
Enable logging by category group for microsoft.network/p2svpngateways to Storage	Monitoring	BuiltIn
Enable logging by category group for Network security groups (microsoft.network/...	Monitoring	BuiltIn
Azure Backup should be enabled for Virtual Machines	Backup	BuiltIn
Configure App Service app slots to use the latest TLS version	App Service	BuiltIn
Enable logging by category group for Service Bus Namespaces (microsoft.serviceb...	Monitoring	BuiltIn
Configure a private DNS Zone ID for table groupID	Storage	BuiltIn
Configure Azure Virtual Desktop workspaces with private endpoints	Desktop Virtualization	BuiltIn
Enable logging by category group for microsoft.timeseriesinsights/environments/e...	Monitoring	BuiltIn
[Preview]: Azure Security agent should be installed on your Windows Arc machines	Security Center	BuiltIn
Azure AI Services resources should restrict network access	Azure Ai Services	BuiltIn
Enable logging by category group for EventGrid Domains (microsoft.eventgrid/do...	Monitoring	BuiltIn
Azure Kubernetes Service Private Clusters should be enabled	Kubernetes	BuiltIn
Enable logging by category group for microsoft.devices/provisioningservices to Lo...	Monitoring	BuiltIn
Enable logging by category group for Azure Database for MySQL servers (microsof...	Monitoring	BuiltIn

Add | Cancel

Створити політику за допомогою порталу

Home > Policy | Assignments >

Assign policy

Basics Advanced **Parameters** Remediation Non-compliance messages Review + create

Search by parameter name

Only show parameters that need input or review

Allowed locations *

West Europe

Home > Policy | Assignments >

Assign policy

Basics Advanced Parameters Remediation Non-compliance messages Review + create

Scope

Scope Learn more about setting the scope *

Azure subscription 1

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition *

Allowed locations for resource groups

Assignment name *

Allowed locations for resource groups

Description

Збережена політика в форматі JSON

Home > Resource groups >

Create a resource group ...

Basics | Tags | Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Project details

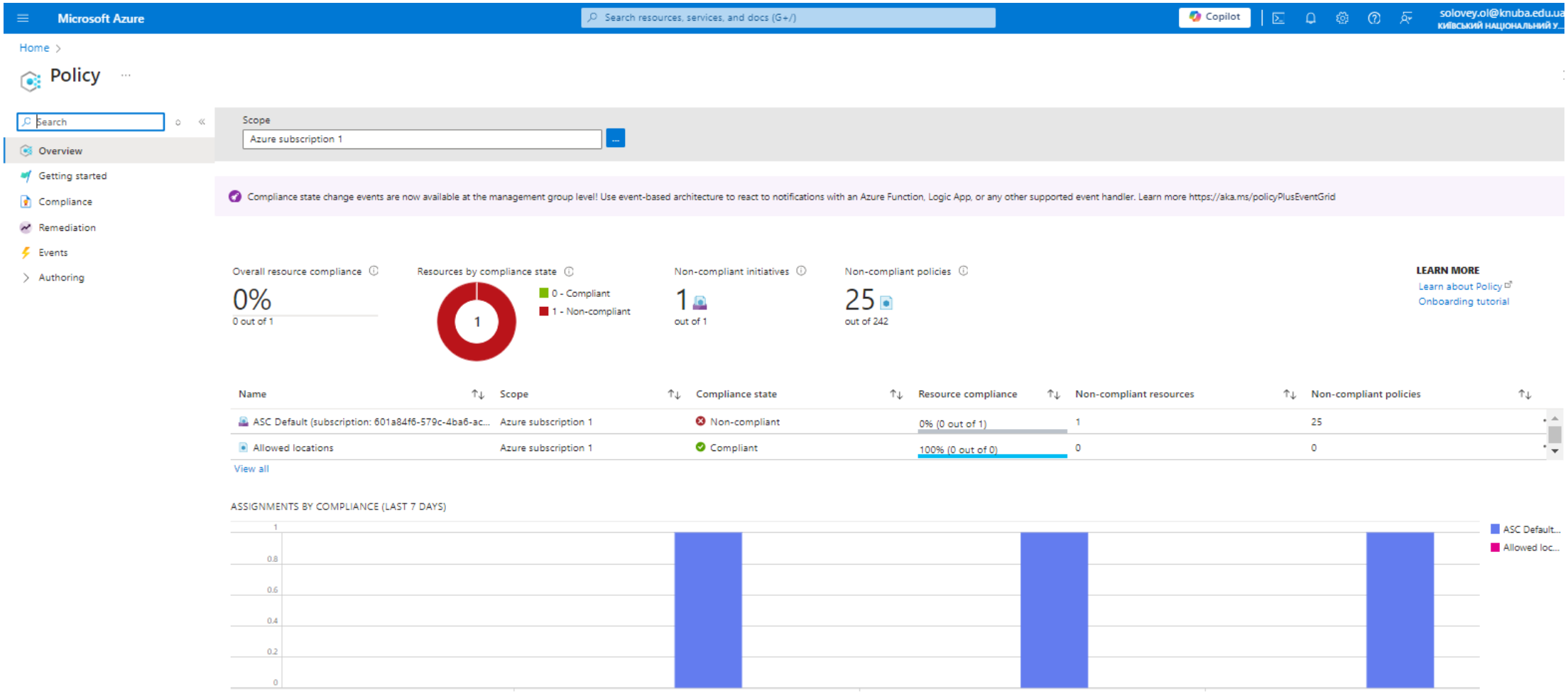
Subscription * : Azure subscription 1

Resource group * : group_for_etl

Resource details

Region * : (US) East US

Policy enforcement. Value does not meet requirements on resource: group_for_etl : Microsoft.Resources/subscriptions/resourceGroups
The value 'eastus' in this field was denied:
Policy e765b5de-1225-4ba3-bd56-1ac6695af988 details



Ресурси, які не відповідають визначеним політикам

Azure Resources

Azure групи ресурсів

Все що ви створюєте в Azure – називається ресурсом. Кожен ресурс має бути включено в групу - 1 група може включати багато ресурсів.

Коли ви застосовуєте дію до групи ресурсів, ця дія буде застосована до всіх ресурсів у групі ресурсів. Якщо ви видалите групу ресурсів, усі ресурси буде видалено. Якщо ви надаєте або забороняєте доступ до групи ресурсів, ви надаєте або забороняєте доступ до всіх ресурсів у групі ресурсів.

Compute Services

У рамках Azure Compute Services включено декілька основних сервісів, які забезпечують обчислювальні ресурси для різних потреб. Ось основні з них:

1. **Virtual Machines (Віртуальні машини)**: Забезпечують масштабовану та на вимогу обчислювальну потужність для запуску додатків та служб.
2. **Azure App Service (Служба додатків Azure)**: Платформа для розміщення веб-додатків, RESTful API та мобільних бекендів з високою доступністю та масштабованістю.
3. **Azure Kubernetes Service (AKS)**: Керована служба Kubernetes для розгортання, управління та роботи з контейнеризованими додатками.
4. **Azure Functions**: Сервіс для виконання коду у відповідь на події без необхідності управління серверами (serverless).
5. **Azure Batch**: Кероване рішення для виконання паралельних та пакетних обчислень у великому масштабі.
6. **Azure Container Instances (ACI)**: Простий та швидкий спосіб запуску контейнерів без необхідності управління інфраструктурою.
7. **Azure Service Fabric**: Платформа для створення та управління масштабованими мікросервісами та контейнерними додатками.
8. **Azure Cloud Services**: Платформа як сервіс (PaaS) для розгортання масштабованих веб-додатків та API.
9. **Azure Dedicated Host**: Фізичні сервери для розміщення ваших віртуальних машин Azure для забезпечення ізоляції на рівні апаратного забезпечення.
10. **Azure Spring Apps**: Повністю кероване середовище для розгортання та управління додатками Spring Boot.

Ці сервіси забезпечують широкий спектр можливостей для розгортання, управління та масштабування додатків та служб у хмарі, забезпечуючи різні сценарії використання, від простих веб-додатків до складних розподілених систем.

Storage Services

У складі Storage Services платформи Azure включено кілька основних сервісів для зберігання даних, кожен з яких призначений для різних типів даних та використання. Ось основні сервіси:

1. **Azure Blob Storage**:
   - **Основне призначення**: Зберігання великих обсягів неструктурованих даних, таких як документи, зображення, відео, резервні копії даних та журнали.
   - **Типи об'єктів**: Block blobs, Append blobs, Page blobs.
2. **Azure File Storage**:
   - **Основне призначення**: Створення повністю керованих файлових спільних ресурсів, які можуть бути доступні через протокол SMB (Server Message Block) для спільного використання файлів між додатками.
   - **Типи сценаріїв**: Спільний доступ до файлів, зберігання конфігурацій додатків, резервне копіювання та відновлення.
3. **Azure Table Storage**:
   - **Основне призначення**: Зберігання великих обсягів структурованих даних з високою масштабованістю. Підходить для таких сценаріїв, як зберігання структурованих даних, журналів подій, даних IoT.
   - **Типи даних**: NoSQL ключ-значення дані.
4. **Azure Queue Storage**:
   - **Основне призначення**: Забезпечення надійного чергового зберігання для великих обсягів повідомлень між компонентами додатків, що працюють асинхронно.
   - **Типи сценаріїв**: Асинхронна передача повідомлень, обробка черг завдань.
5. **Azure Disk Storage**:
   - **Основне призначення**: Забезпечення високопродуктивного керованого дискового зберігання для віртуальних машин (VMs) з різними рівнями продуктивності (Standard HDD, Standard SSD, Premium SSD, Ultra Disk).
   - **Типи дисків**: OS disks, Data disks.
6. **Azure Archive Storage**:
   - **Основне призначення**: Зберігання даних, які рідко використовуються, але які потрібно зберігати на довгий термін. Підходить для архівування, резервного копіювання та зберігання даних відповідно до вимог регуляторів.
   - **Типи даних**: Неактивні дані, архівні дані.

Database Services

До категорії Database Services на платформі Azure включені наступні сервіси:

1. **Azure SQL Database**:
   - Керована реляційна база даних як сервіс (DBaaS) з вбудованими можливостями для високої доступності, автоматичного масштабування, резервного копіювання та безпеки.
2. **Azure Cosmos DB**:
   - Глобально розподілена, багатомодельна база даних, яка забезпечує високу доступність, низьку затримку та горизонтальне масштабування для різних моделей даних, таких як документи, ключ-значення, графи та стовпці.
3. **Azure Database for MySQL**:
   - Керована служба бази даних MySQL з вбудованими можливостями для високої доступності, резервного копіювання та безпеки.
4. **Azure Database for PostgreSQL**:
   - Керована служба бази даних PostgreSQL з можливостями для масштабування, високої доступності та забезпечення безпеки.
5. **Azure Database for MariaDB**:
   - Керована служба бази даних MariaDB з вбудованими функціями для резервного копіювання, відновлення, безпеки та масштабування.
6. **SQL Managed Instance**:
   - Повністю керований інстанс SQL Server, який забезпечує повну сумісність з локальним SQL Server та вбудованими можливостями для високої доступності, резервного копіювання та безпеки.
7. Azure Synapse Analytics (раніше SQL Data Warehouse):
   - Інтегрована аналітична служба, яка об'єднує можливості аналізу великих даних і зберігання даних, забезпечуючи масштабовану аналітику.
8. **Azure Cache for Redis**:
   - Керована служба кешування на основі Redis, яка забезпечує високу продуктивність, масштабованість та підтримку для тимчасового зберігання даних.
9. **Azure SQL Edge**:
   - Версія SQL Server, оптимізована для пристроїв Інтернету речей (IoT), яка забезпечує можливості для зберігання та аналізу даних на периферії.

Networking Services

В Networking Services на платформі Azure включено кілька ключових сервісів, які забезпечують підключення, управління та захист мережевої інфраструктури. Ось основні з них:

1. **Virtual Network (VNet)**:
   - Забезпечує ізольовані мережі для захищеного підключення та управління ресурсами Azure.
2. **Azure Load Balancer**:
   - Розподіляє вхідний мережевий трафік між кількома віртуальними машинами для забезпечення високої доступності.
3. **Azure Application Gateway**:
   - Забезпечує маршрутизацію на рівні додатків і балансування навантаження, включаючи функціонал веб-аплікаційного фаєрволу (WAF).
4. **Azure DNS**:
   - Хостинг і управління DNS доменами та записами.
5. **Azure Traffic Manager**:
   - Розподіл трафіку на основі географічного розташування або інших параметрів для забезпечення високої доступності та продуктивності.
6. **Azure VPN Gateway**:
   - Захищене підключення між локальними мережами та Azure через VPN.
7. **Azure ExpressRoute**:
   - Пряме підключення до Azure з локальних мереж через приватне з'єднання, минаючи Інтернет.
8. **Azure Front Door**:
   - Глобальне балансування навантаження та CDN для оптимізації доставки контенту і підвищення продуктивності додатків.
9. **Azure Bastion**:
   - Безпечний віддалений доступ до віртуальних машин без відкриття публічних IP-адрес.
10. **Azure Firewall**:
    - Керований хмарний фаєрвол для захисту мережевих ресурсів.
11. **Azure DDoS Protection**:
    - Захист від розподілених атак типу "відмова в обслуговуванні" (DDoS).
12. **Azure Private Link**:
    - Безпечне підключення до Azure служб через приватний кінцевий пункт віртуальної мережі.

Security Services

Сервіси, які включені в категорію **Security Services** на платформі Azure, забезпечують захист і управління безпекою для ваших ресурсів. Основні сервіси включають:

Azure Active Directory (AAD): Служба управління ідентифікацією та доступом для користувачів та додатків. Включає функції єдиного входу (SSO), багатофакторної автентифікації (MFA) та управління ідентифікаціями.

Azure Key Vault: Безпечне зберігання та управління ключами шифрування, сертифікатами та секретами (паролі, ключі доступу та інші конфіденційні дані).

Azure Security Center: Централізоване управління безпекою та захист від загроз для гібридних робочих навантажень. Дозволяє оцінювати стан безпеки, виявляти та реагувати на загрози.

Azure Firewall: Керований хмарний сервіс брандмауера, що забезпечує захист мережевих ресурсів. Пропонує функції фільтрації трафіку, захисту від загроз та управління правилами безпеки.

Azure DDoS Protection: Захист від атак типу "відмова в обслуговуванні" (DDoS), який забезпечує автоматичне виявлення та пом'якшення атак на ваші додатки та сервіси.

Azure Information Protection (AIP): Сервіс для класифікації, маркування та захисту даних, допомагає контролювати доступ до конфіденційної інформації.

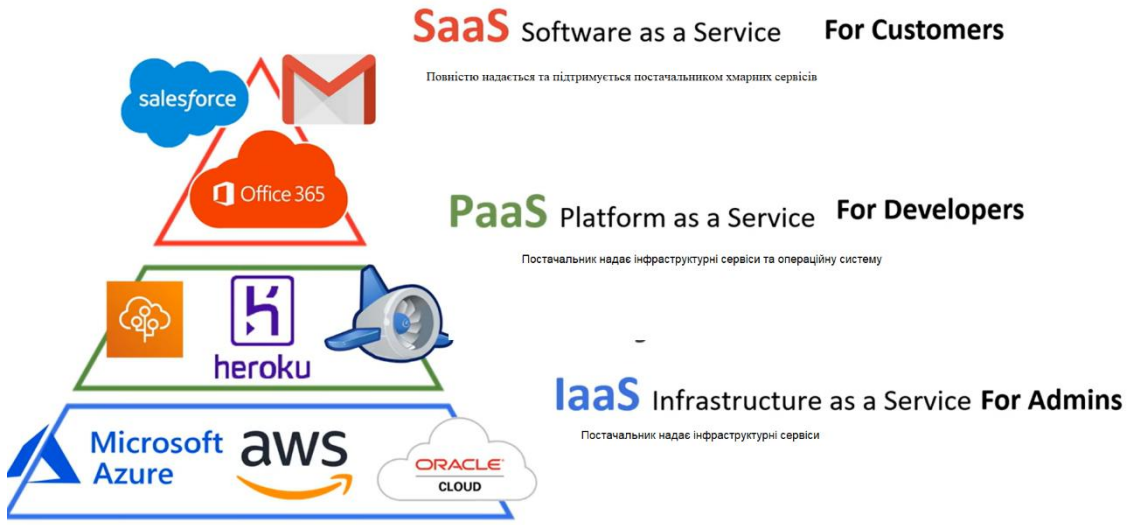
Microsoft Defender for Cloud: Комплексне рішення для захисту робочих навантажень у хмарі, включаючи виявлення загроз, аналіз вразливостей та пропозиції щодо покращення безпеки.

Microsoft Defender for Identity: Виявлення та розслідування передових атак, компрометацій облікових записів та інсайдерських загроз в локальних і хмарних середовищах.

Microsoft Sentinel: Хмарна система управління інформацією про безпеку та події (SIEM), що забезпечує інтелектуальне виявлення загроз та реагування.

Azure Policy: Дозволяє створювати та застосовувати політики для забезпечення відповідності та управління ресурсами в Azure

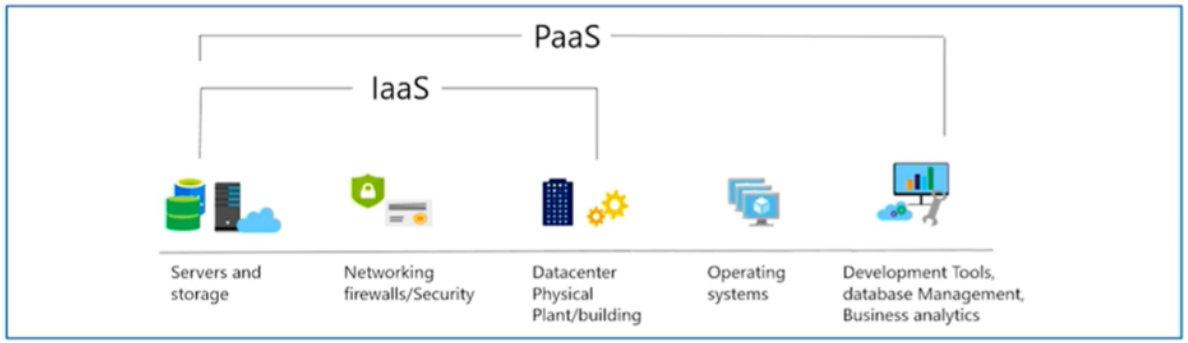
Моделі хмарних обчислень



Інфраструктура як послуга (IaaS) - постачальник хмарних служб надає: ВМ (сервер), Мережу і будівлю в який знаходиться сервер (центр обробки даних - datacenter).

Platform as a Service (PaaS)

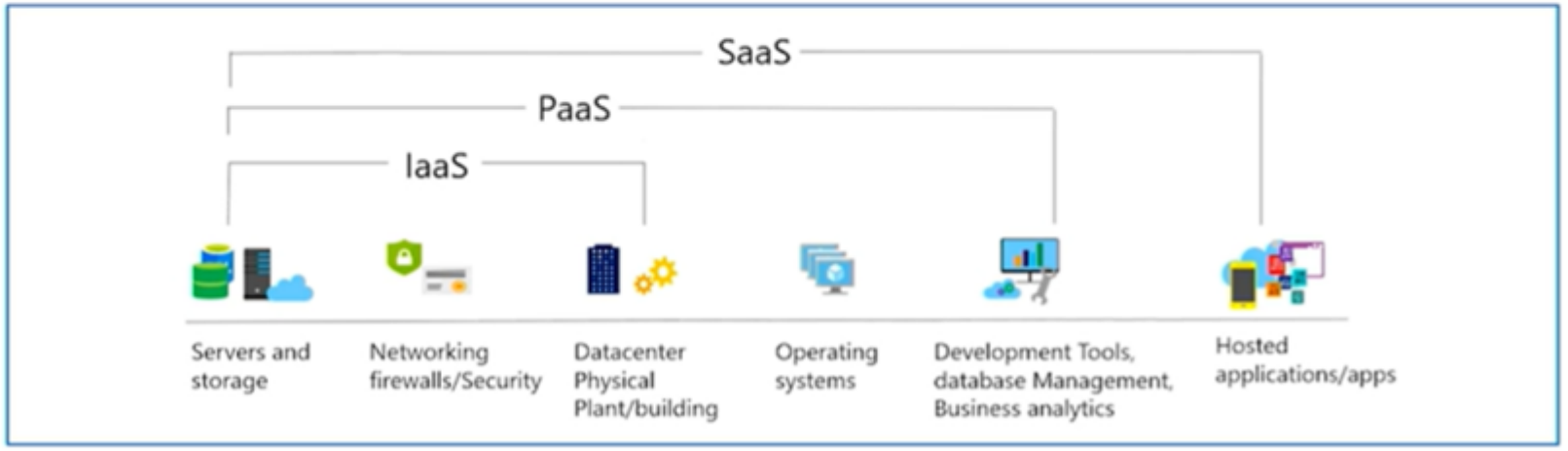
Provides environment for building, testing, and deploying software applications; without focusing on managing underlying infrastructure.



Платформа як послуга (PaaS) - постачальник хмарних служб надає: сховище, SQL базу даних, App Service - Операційну систему, систему управління базами даних, інструменти для розробки.

Software as a Service (SaaS)

Users connect to and use cloud-based apps over the internet: for example, Microsoft Office 365, email, and calendars.

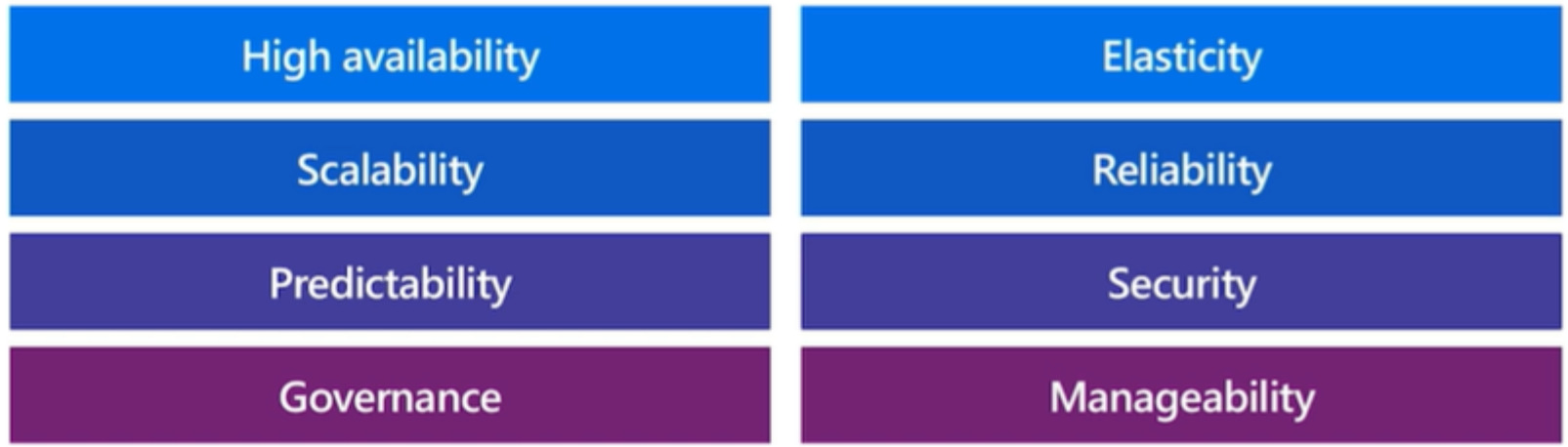


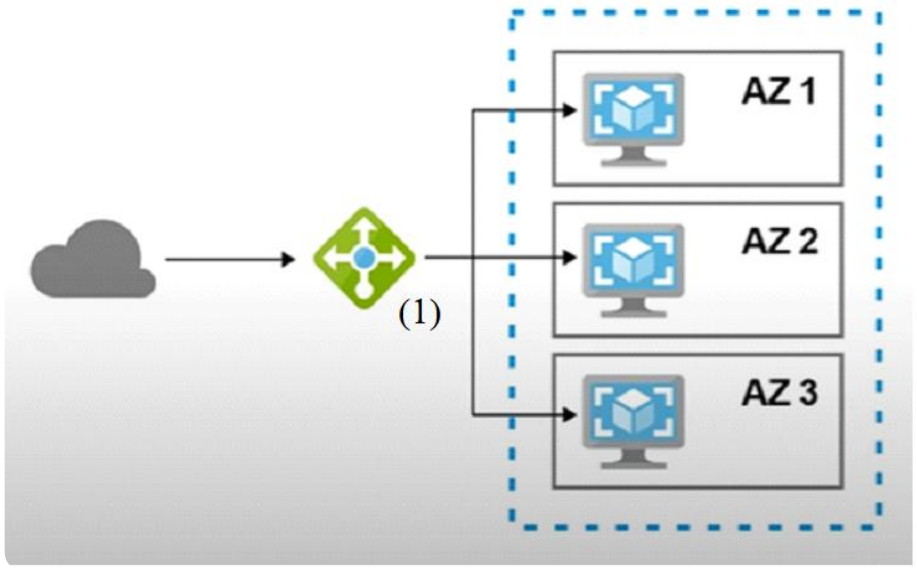
Програмне забезпечення як послуга (SaaS) – це найбільш повна модель хмарної служби з погляду продукту. При використанні SaaS ви, по суті, орендуєте або використовуєте повністю розроблений додаток.

Розподіл відповідальності для моделей хмарних обчислень

Локальний сервер	IaaS	PaaS	SaaS
Програмні доданки	Програмні доданки	Програмні доданки	Програмні доданки
Облікові записи	Облікові записи	Облікові записи	Облікові записи
Виконання програмних доданків	Виконання програмних доданків	Виконання програмних доданків	Виконання програмних доданків
Інфраструктура (middleware)	Інфраструктура (middleware)	Інфраструктура (middleware)	Інфраструктура (middleware)
Операційна мережа	Операційна мережа	Операційна мережа	Операційна мережа
Віртуалізація	Віртуалізація	Віртуалізація	Віртуалізація
Сервери	Сервери	Сервери	Сервери
Збереження	Збереження	Збереження	Збереження
Мережа	Мережа	Мережа	Мережа

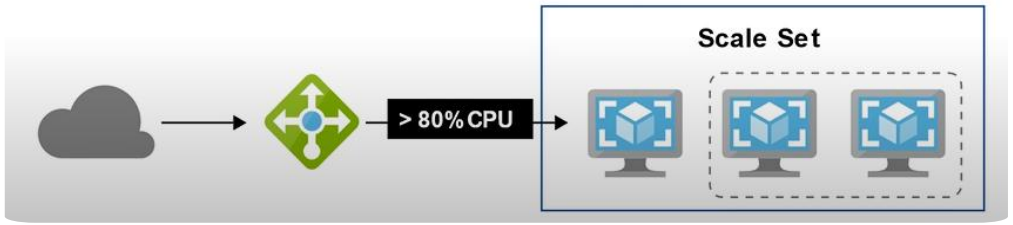
Основні архітектурні рішення «хмари»



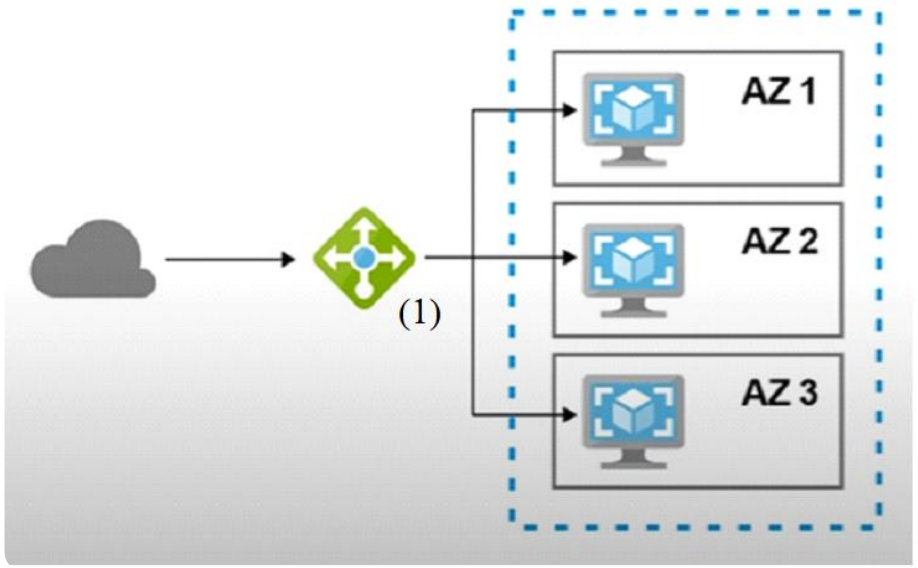


❖*Висока доступніть і надійність (High availability and reliability)*–забезпечується наявність більш ніж 1-го сервера в **різних доступних зонах (AZ),** та переключенні з 1-го на інший сервер у випадку необхідності. Доступна зона – це місце фізичного розташування центру обробки даних (datacenter). Центр обробки даних – це будівля, яка вміщає 1000 комп'ютерів. Трафік розподіляється в вузлі розподілу навантаження (1).

Еластичність (Elasticity)

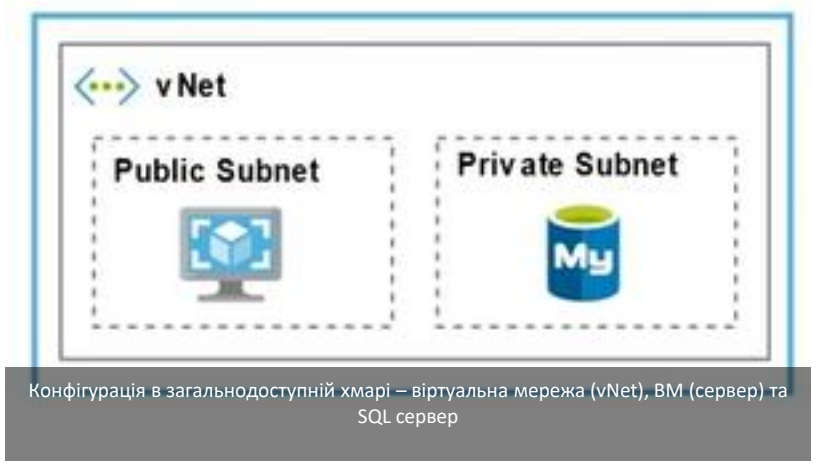


- Еластичність (Elasticity) – автоматично зменшує/збільшує виділені ресурси залежно від навантаження. Еластичність досягається рішенням «масштабовані набори» (scale sets).
  - За допомогою масштабованих наборів ви створюєте модель конфігурації віртуальної машини, яка автоматично додаєте або видаляєте додаткові екземпляри на основі завантаження ЦП або пам'яті або завантаження мережі.
  - Наприклад, ви можете зробити конфігурацію відповідно якої при завантаження ЦП біль ніж на 80% - має відбутися горизонтальне масштабування з 1-го до 3-х серверів; і при навантажені менш ніж 80% - знов повернутись до 1 сервера.
- Fault Tolerance – здатність підтримувати ВМ та інші ресурси у робочому стані у випадку не доступності центру даних. (Відмовостійкість: програма має продовжувати працювати належним чином навіть за наявності апаратних або програмних збоїв.)
- Disaster Recovery – здатність усувати та передбачати аварії пов’язані з технологією. Забезпечується резервним копіюванням даних.



- *Висока масштабованість (High Scalability)* – надає необхідні ресурси при збільшені навантаження. У разі необхідності виконуються перехід або на більш потужний сервер (1) – вертикальне масштабування або на декілька серверів тієї ж потужності – горизонтальне масштабування.

Моделі розгортання хмарних обчислень. Публічна хмара (Public cloud)



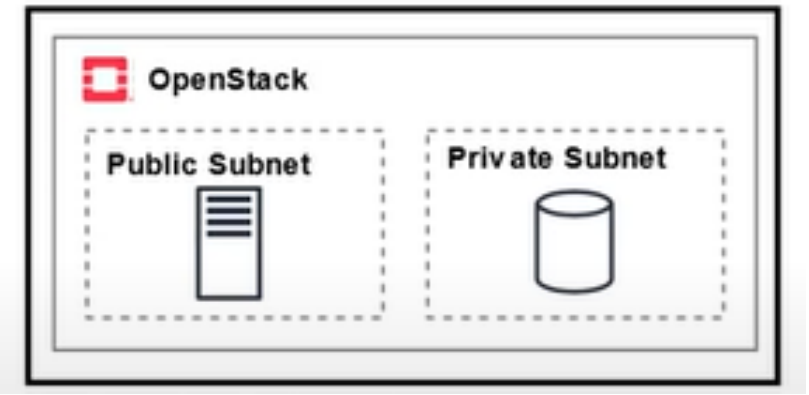
Конфігурація в загальнодоступній хмарі – віртуальна мережа (vNet), ВМ (сервер) та SQL сервер

- *Загальнодоступні хмари* є стандартним способом розгортання хмарних обчислень. Хмарні ресурси (наприклад, сервери та сховища) належать сторонньому постачальнику хмарних служб, який управляє ними, і передаються через Інтернет. У загальнодоступній хмарі ви використовуєте те саме обладнання, сховище та мережеві пристрої спільно з іншими організаціями або хмарними клієнтами. Ви отримуєте доступ до служб і керуєте своїм обліковим записом через веб-браузер. Розгортання загальнодоступних хмар часто використовуються для надання інтернет-служби електронної пошти, програм Office в Інтернеті, сховищ та середовищ тестування та розробки.

- Переваги загальнодоступних хмар:

• **Економія**. Вам не потрібно придбати обладнання або програмне забезпечення. Ви платите лише за службу, що використовується.
• **Відсутність потреби у підтримці інфраструктури**. Ці завдання перебирає постачальник служби.
• **Майже необмежена масштабованість**. Вам надаються ресурси на вимогу, які задовольняють потреби вашої компанії.
• **Висока надійність**. Велика мережа серверів забезпечує захист від збоїв.
• До популярних публічних хмарних постачальників належать Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud та інші.

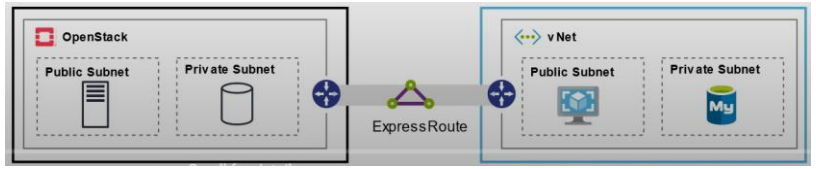
Приватна хмара (Private Cloud)



OpenStack рішення для створення хмарного середовища в локальному центрі обробки даних

- *Приватна хмара* складається з хмарних обчислювальних ресурсів, які використовує лише одна компанія чи організація. Архітектура приватної хмари відрізняється використанням **OpenStack** - програмного забезпечення для створення обчислювальних хмар і хмарних сховищ для забезпечення внутрішніх потреб компанії. Приватна хмара може бути фізично розташована **в локальному центрі обробки даних організації** або розміщена у стороннього постачальника служб. Однак у приватній хмарі служби та інфраструктура завжди розміщені у приватній мережі, а апаратне та програмне забезпечення призначене виключно для вашої організації. Приватні хмари часто використовуються державними органами, фінансовими установами та будь-якими іншими організаціями середнього та великого розміру з важливими для бізнесу операціями, які хочуть підвищити рівень контролю за своїм середовищем.
- Переваги приватної хмари:
- **Більше гнучкості**. організація може налаштувати своє хмарне середовище для задоволення конкретних бізнес-потреб.
- **Більше контролю**. До ресурсів не надається загальний доступ, тому забезпечується високий рівень контролю та конфіденційності.
- **Вища масштабованість**. Приватні хмари нерідко забезпечують більшу масштабованість у порівнянні з локальною інфраструктурою.

Гібридна хмара



- *Гібридна хмара* – це тип хмарних обчислень, у яких локальна інфраструктура (або приватна хмара) поєднується із загальнодоступною хмарою. Гібридні хмари дозволяють переміщати дані та програми між двома середовищами. Для підключень з приватного хмарного середовища до загального використовується рішення – ExpressRoute. пропускна спроможність каналу *ExpressRoute* - дуплексна. Наприклад, якщо ExpressRoute 200 Мбіт/с, значить - 200 Мбіт/с для вхідного трафіку і 200 Мбіт/с для вихідного трафіку.
- Переваги гібридної хмари:
- **Контроль**. Організація може підтримувати приватну інфраструктуру для важливих ресурсів або робочих навантажень, для яких потрібна низька затримка.
- **Гнучкість**. Ви можете використовувати додаткові ресурси у загальнодоступній хмарі, коли вони вам знадобляться.
- **Економічність**.

	Вартість	Безпека	Конфігурація	Вимоги щодо технічних знань користувачів
Публічна хмара	Економічно ефективна	Надаються базові послуги з безпеки	Обмежена, тим що постачальник хмарних послуг пропоную. Додавати особисто нічого не можливо	Не вимагає поглиблених тех знань
Приватна хмара (Private Cloud)	великі фінансові витрати	Послуги з безпеки надаються відповідно вимогам користувачів	Користувачі отримають конфігурацію відповідно їх вимогам	Необхідні Техн знання щодо конфігурації інфраструктури
Гібридна хмара	Може бути досить економічною	Послуги з безпеки надаються відповідно вимогам користувачів	Користувачі отримають конфігурацію відповідно їх вимогам	Необхідні Техн знання щодо конфігурації інфраструктури

Питання

1. Які основні можливості надає Microsoft Azure як платформа віртуалізації?
2. У чому різниця між IaaS, PaaS та SaaS у контексті Azure?
3. Які типи віртуальних машин доступні в Azure, і як відрізняються їхні сценарії використання?
4. Які переваги має хмарна віртуалізація Azure порівняно з локальною інфраструктурою?
5. Як Azure забезпечує високу доступність і масштабованість віртуалізованих ресурсів?
6. Що таке Azure Resource Manager і яку роль він відіграє в керуванні ресурсами Azure?
7. Що таке ARM-шаблон, і в яких випадках його застосовують?
8. Як ARM забезпечує контроль доступу та безпеку під час роботи з ресурсами?
9. У чому переваги декларативного підходу розгортання ресурсів через ARM порівняно з імперативним?
10. Як ARM Groups (Resource Groups) впливають на структуру та організацію ресурсів у підписці Azure?
11. Що вважається ресурсом у Microsoft Azure та які основні категорії ресурсів існують?
12. Які залежності можуть виникати між різними ресурсами Azure (наприклад, VM, Storage, Network)?
13. Яку інформацію зазвичай містить Resource ID, і чому він є важливим для роботи з Azure API?
14. Як працює система тегів (Tags) для ресурсів Azure та які завдання вона допомагає вирішувати?
15. Яким чином Azure забезпечує моніторинг і діагностику ресурсів через такі інструменти, як Azure Monitor та Log Analytics?