Лекція 2.

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.

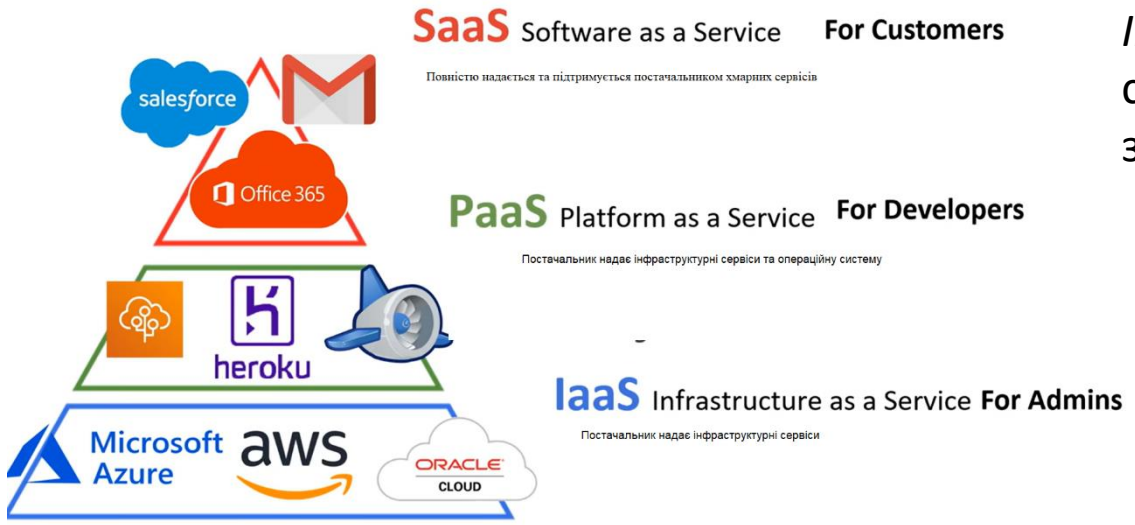
Microsoft Defender for Cloud: Комплексне рішення для захисту робочих навантажень у хмарі, включаючи виявлення загроз, аналіз вразливостей та пропозиції щодо покращення безпеки.

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

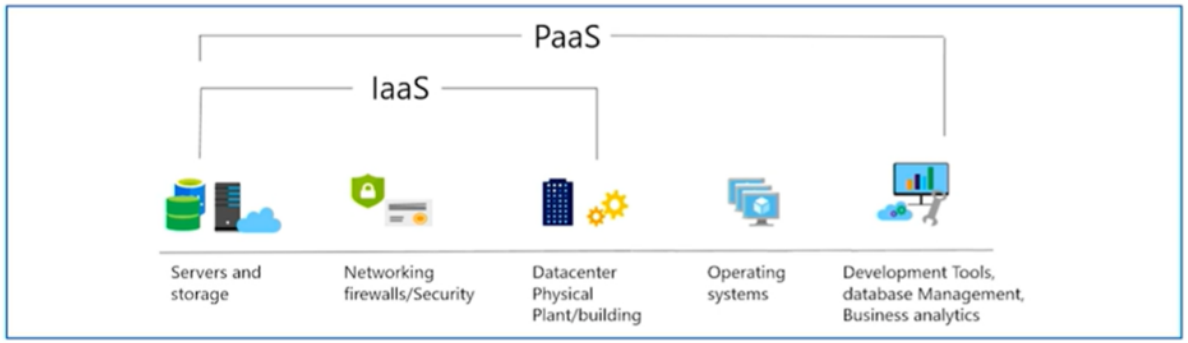
Моделі хмарних обчислень



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)

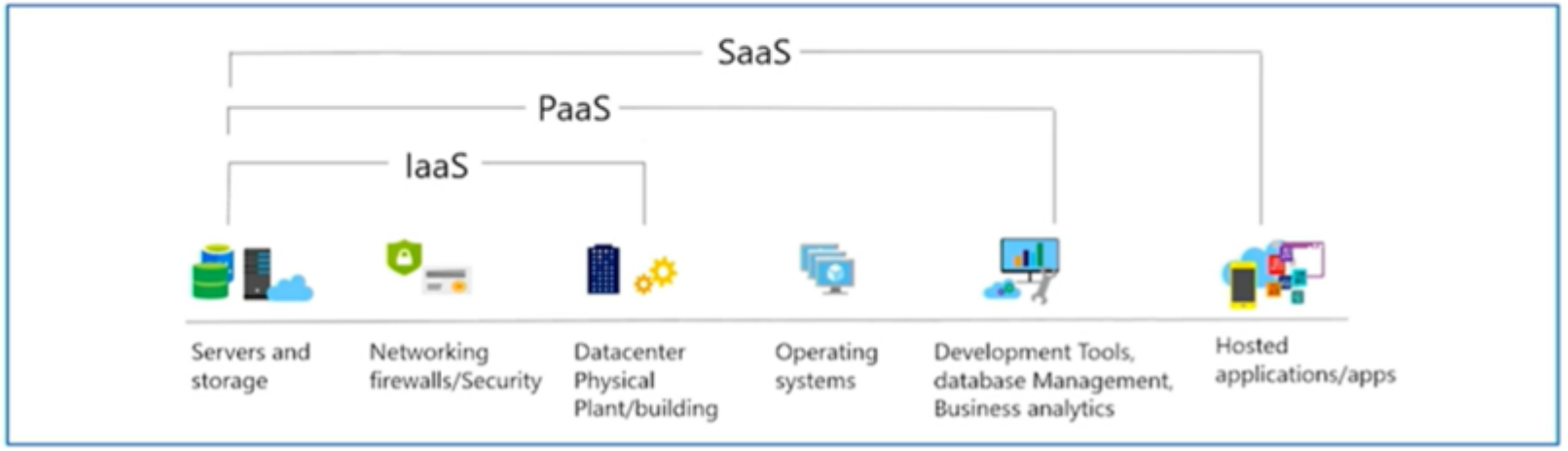
Provides environment for building, testing, and deploying software applications; without focusing on managing underlying infrastructure.



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.

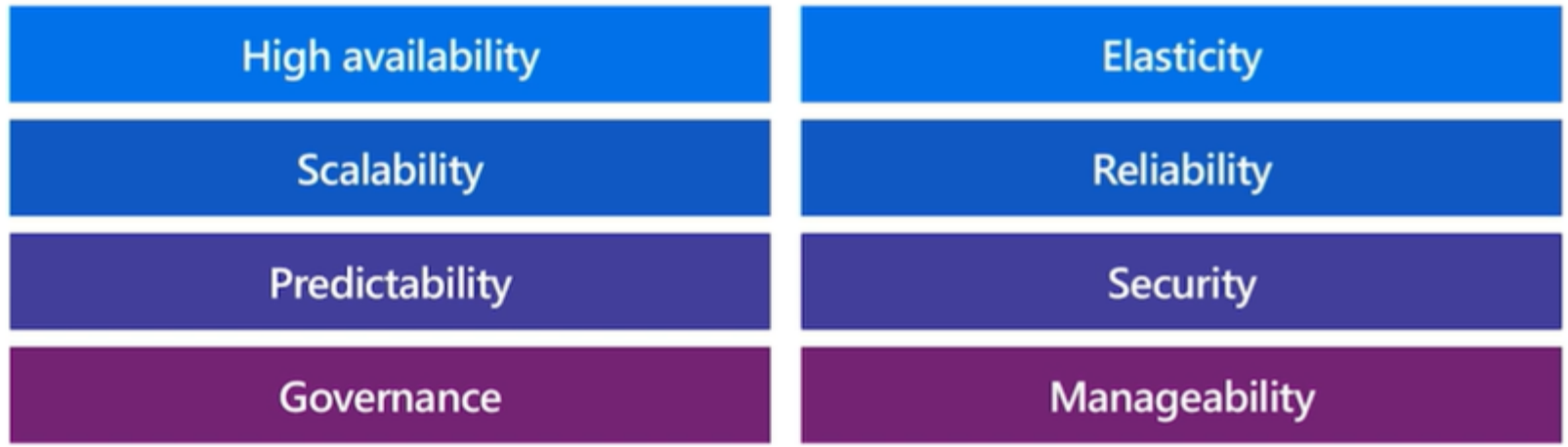


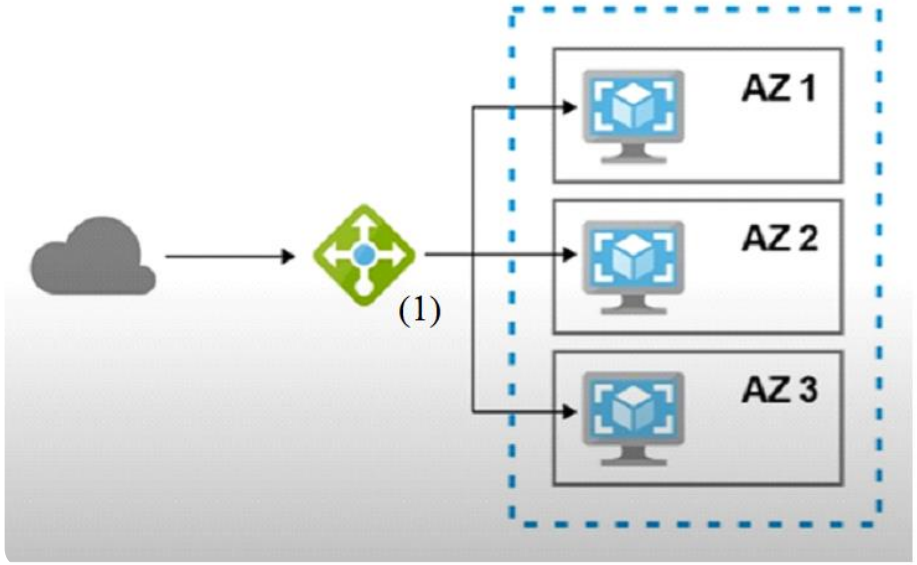
Програмне забезпечення як послуга (SaaS) – це найбільш повна модель хмарної служби з погляду продукту. При використанні SaaS ви, по суті, орендуєте або використовуєте повністю розроблений додаток.

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

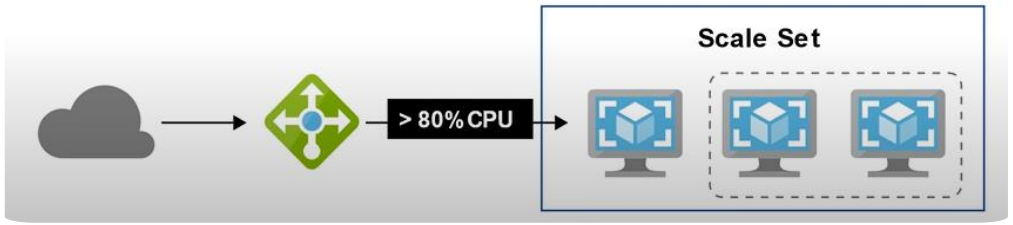
Основні архітектурні рішення «хмари»



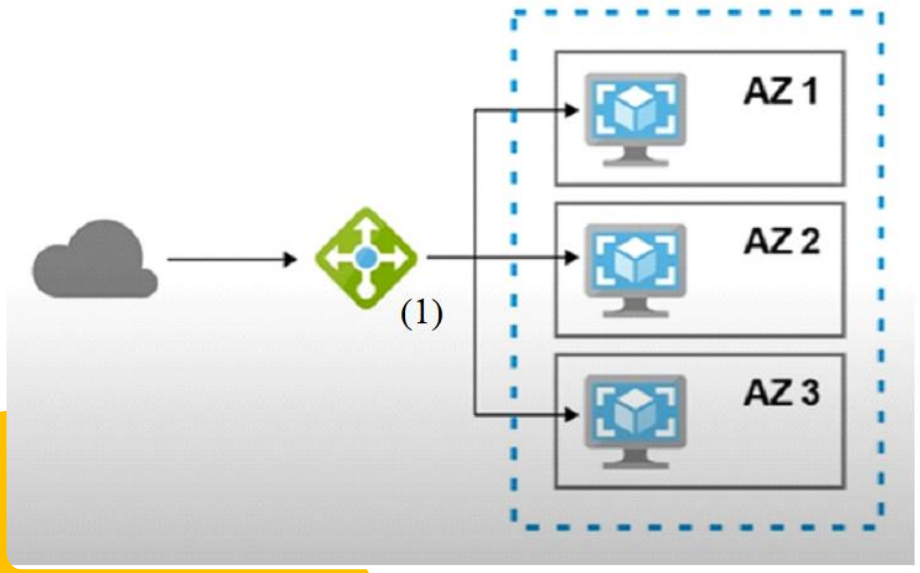


❖*Висока доступніть і надійність (High availability and reliability)*–забезпечується наявність більш ніж 1-го сервера в **різних доступних зонах (AZ),** та переключенні з 1-го на інший сервер у випадку необхідності. Доступна зона – це місце фізичного розташування центру обробки даних (datacenter). Центр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

Еластичність (Elasticity)

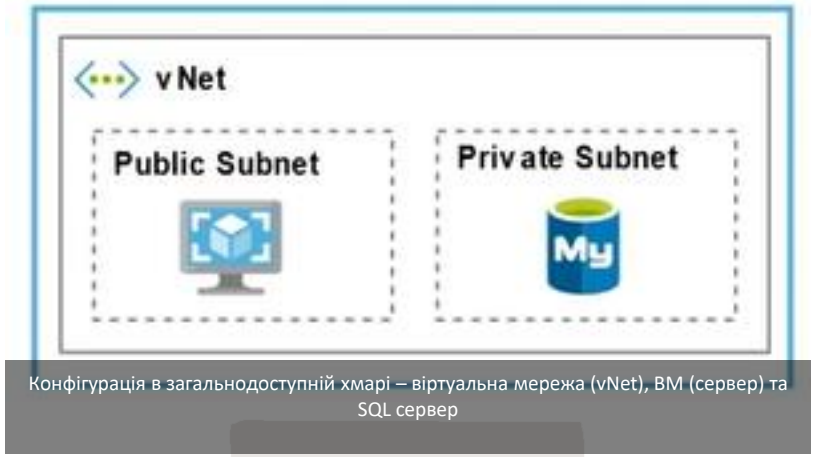


- Еластичність (Elasticity) – автоматично зменшує/збільшує виділені ресурси залежно від навантаження. Еластичність досягається рішенням «масштабовані набори» (scale sets).
  - За допомогою масштабованих наборів ви створюєте модель конфігурації віртуальної машини, яка автоматично додаєте або видаляєте 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)



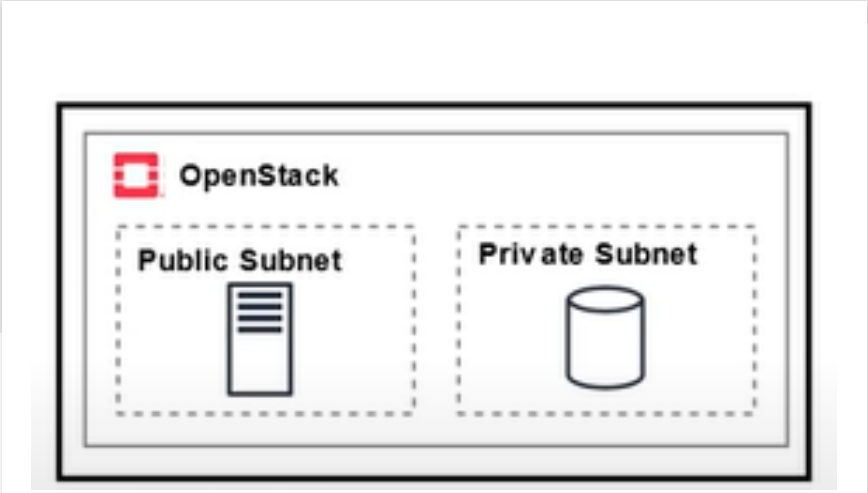
Конфігурація в загальнодоступній хмарі – віртуальна мережа (vNet), ВМ (сервер) та SQL сервер

- *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.

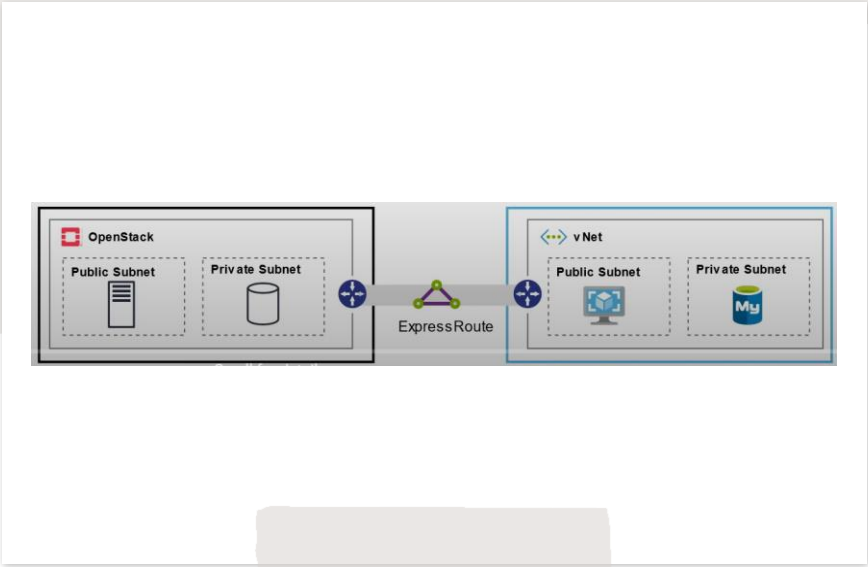
Приватна хмара (Private Cloud)



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**.

Моделі хмарних обчислень

	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 сервіси включено в модель IaaS?
2. Які основні архітектурні рішення «хмари»?
3. При якій моделі розгортання хмарних обчислень організації самі контролюють безпеку?
4. Яка модель хмарних технологій IaaS, PaaS, SaaS потребує найбільшого керування користувачами хмарних служб?
5. До якої моделі хмарних технологій IaaS, PaaS, SaaS належить Cosmos DB?
6. Після міграції в хмару за моделлю SaaS чи має користувач проводити оновлення програмного забезпечення?
7. Після міграції в хмару за моделлю IaaS чи має компанія самостійно розгортати необхідне програмне забезпечення?
8. Після міграції в «Загальну», «Приватну» чи «Гібритну» хмару організації більше не потребуватиме в локальному центрі обробки даних?
9. Ви маєте ВМ в хмарі, хто Ви чи постачальних «хмарних послуг» відповідає за: налаштування та керування ВМ?
10. Чи має користувач повний контроль на ОС в моделі PaaS?
11. При провадженні рішення SaaS, чи має користувач виконати конфігурацію та налаштування SaaS?
12. В чому різниця між рекомендованими та альтернативними регіонами?
13. Яке рішення у випадку «аварійного відновлення» використається Azure?

Основи функціонування центрів обробки даних (ЦОД)

Ucloud

EQUINIX

DIGITAL REALTY

中国电信 CHINA TELECOM

NTT Communications

verizon

Лекція 2

tucha Хмарні рішення

Volia data center

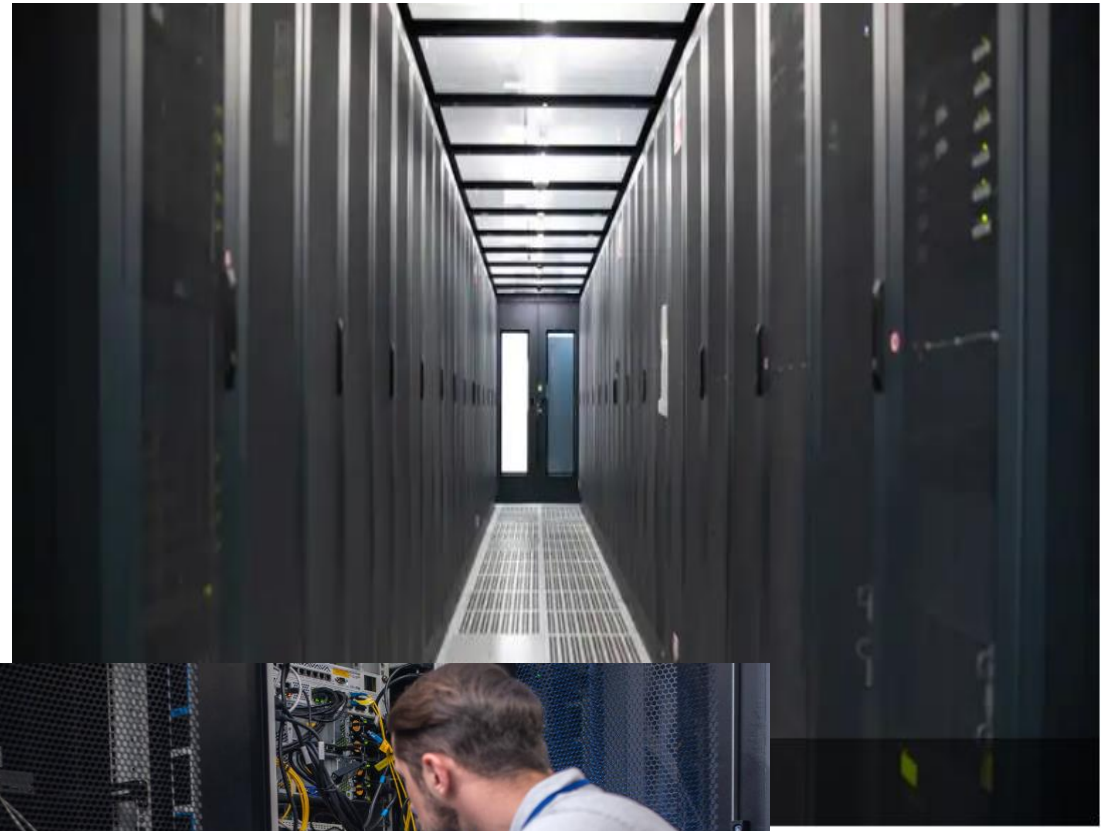
Хмарні сервіси для повноцінної роботи вимагають наявності спеціальної серверної інфраструктури, яку найпростіше забезпечити за допомогою так званих дата-центрів (синонім — ЦОД або центр обробки даних).

Дата-центр — це центр обробки даних (ЦОД), спеціальна будівля, в якій знаходиться серверне та мережеве обладнання для підключення користувачів до інтернет-каналів. У цьому місці зберігаються, обробляються та передаються дані бізнесу, а також інформація для особистого користування клієнтів, яка розміщена на їхньому обладнанні. Розміри дата-центрів дуже відрізняються. Бувають зовсім маленькі, які вміщаються у вантажний контейнер і можуть переїжджати, а бувають величезні приміщення площею в тисячі квадратних метрів.

Хмарні центри обробки даних — це тип центрів обробки даних, призначених для підтримки хмарних обчислень. Вони мають високу масштабованість і можуть використовуватися для підтримки широкого діапазону програм і робочих навантажень. Хмарні центри обробки даних часто використовують технологію віртуалізації, щоб забезпечити ефективне використання обчислювальних ресурсів.

У світі є мільйони дата-центрів. Вони зберігають та обробляють трильйони гігабайт інформації. Серед неї — фільми в онлайні, книги у додатку, ігри у браузері, безліч програм, фінансових даних та інше. Дата-центри мають великий вплив на наше життя та взаємодію з віртуальним світом.

Розміри дата-центрів, їх зовнішній вигляд та оснащеність технологіями дуже відрізняються. За даними Cisco, в середньому в одному з них обробляються мільярди гігабайт інформації і надходять сотні мільйонів мегабайт нової. І це лише за добу. При цьому будь-який якісний дата-центр відповідає за безперервний час доступності сервера (аптайм), який дозволяє, наприклад, вашому сайту бути доступним 24/7 (за умови наявності інтернет-каналу до вашого сервера, а краще двох каналів).



Центри Обробки Даних дозволяють централізувати потужності для зберігання та обробки інформації, підвищити безпеку, надійність роботи, швидкість доступу до інформації та швидкість її обробки.

Основними критеріями при створенні даних систем, з точки зору обробки і зберігання інформації, є:

- **Функціональність ЦОД** – здатність централізовано забезпечувати заданий набір IT-сервісів з приймання, обробки, зберігання та надання інформації користувачам.
- **Доступність ресурсів ЦОД** – гарантоване надання необхідних обчислювальних ресурсів ЦОД в потрібний час.
- **Достовірність і безпеку даних в ЦОД** –забезпечення достовірності та цілісності даних, що є важливим завданням для більшості інформаційних систем.
- **Продуктивність і масштабованість ЦОД** – можливість збільшення обсягів даних і нарощування обчислювальної потужності для надійної роботи системи в умовах зростаючого навантаження, внаслідок підвищення обсягів і складності оброблюваних задач.
- **Керованість і повнота використання ресурсів** – для вирішення цього завдання використовуються технічні засоби управління навантаженням і організаційні заходи, що забезпечують максимальне завантаження обчислювальних ресурсів.
- **Сукупна вартість володіння** –це методика, призначена для визначення витрат на інформаційні системи, які розраховуються на всіх етапах життєвого циклу системи. Сукупна вартість володіння ЦОД в півтора-два рази нижче, в порівнянні з децентралізованими системами обробки даних.

Приклад ЦОД

ЦОД, або дата-центри відповідають за безперебійну роботу всього встановленого всередині обладнання та відповідної інфраструктури. Простими словами ЦОД – це не стільки центр обробки даних, скільки місце для розміщення обладнання.

Приміщення ЦОД найчастіше розміщують біля точки обміну трафіком, оскільки доступ до обчислювального устаткування дата-центру найчастіше здійснюється через інтернет. Оснащують його сучасними ефективними інженерними системами – це запорука стабільного функціонування.

Водночас ЦОД повинен бути забезпечений сучасними системами резервування енергії, пожежогасіння та низкою інших важливих вузлів, рівень яких підтверджується відповідним сертифікатом, а якість і обсяг послуг, що надаються можуть бути дуже різними.

Дата-центр Dattum у Ризі Латвія / Фото Tet

Електропостачання

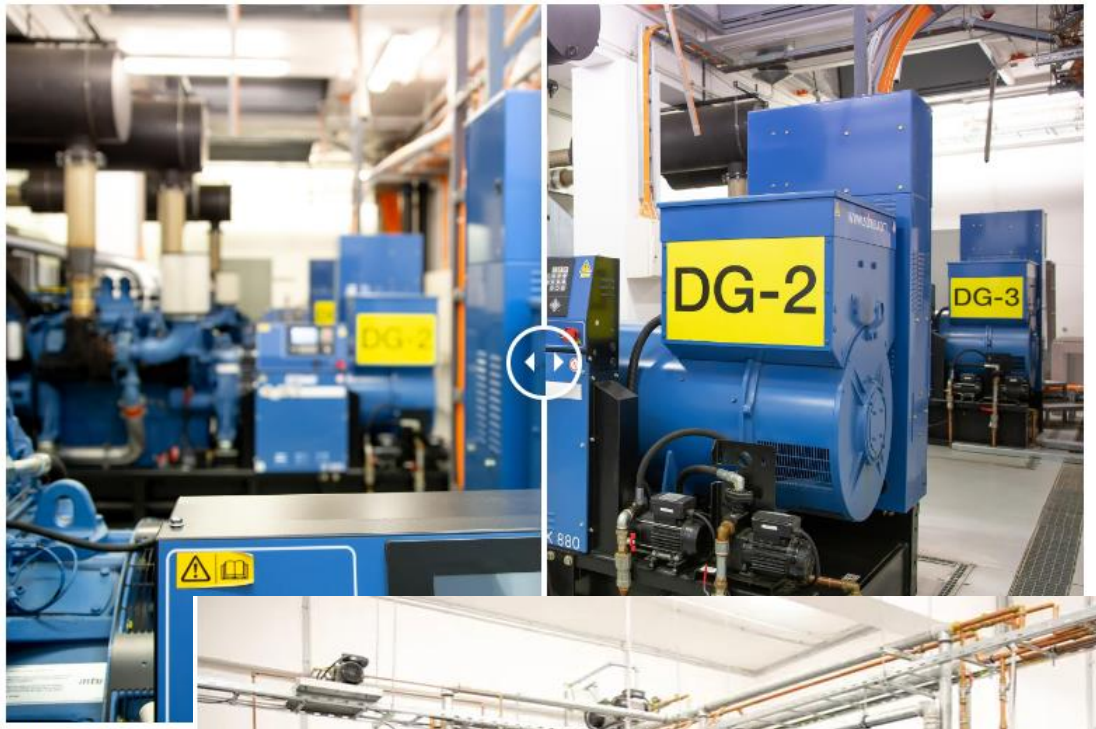
Головне джерело життя ЦОД – електрика. Від того, наскільки правильно і безперебійно здійснюється електроживлення дата-центру, залежить стабільність роботи розміщеного в ньому обладнання. Тому ЦОД підключають до електромережі по декількох незалежних каналах, встановлюють системи безперебійного живлення, а також підключають додатковий дизельний генератор (або кілька) на випадок повного відключення електрики.

Акумулятори та системи безперебійного живлення дають змогу уникнути різких перепадів та вимкнень енергії та слугують одним з дублюючих джерел живлення на випадок відключення електрики. Їхня мета, забезпечити роботу ЦОД до запуску дизельних генераторів.

Акумулятори в Dattum забезпечують безперебійну роботу / Фото Тет

Ресурс батарей в дата-центрі Dattum (300 акумуляторів) дає змогу підтримувати роботу ЦОД протягом 30 хвилин – цього достатньо аби запрацювали три дублюючі дизельні генератори. Генератори (3х0,88 МВт), які працюють на дизельному пальному облаштовані у спеціальному приміщенні, яке має автоматизовану систему люків, що слугують протипожежною системою за принципом вакууму. Водночас в підлогу вмонтована спеціальна струна, яка реагує у випадку протікання пального. В такому випадку на системах адміністрування вказується сектор та конкретне місце протікання, що дозволяє швидко зреагувати на інцидент.

Усі системи перевіряють та регулярно тестуються у тестовому режимі, аби у будь-який момент все було в робочому стані для забезпечення безперебійної роботи ЦОД. Обидві генераторні системи запускаються та синхронізуються протягом 30 секунд.



Дизельні ге

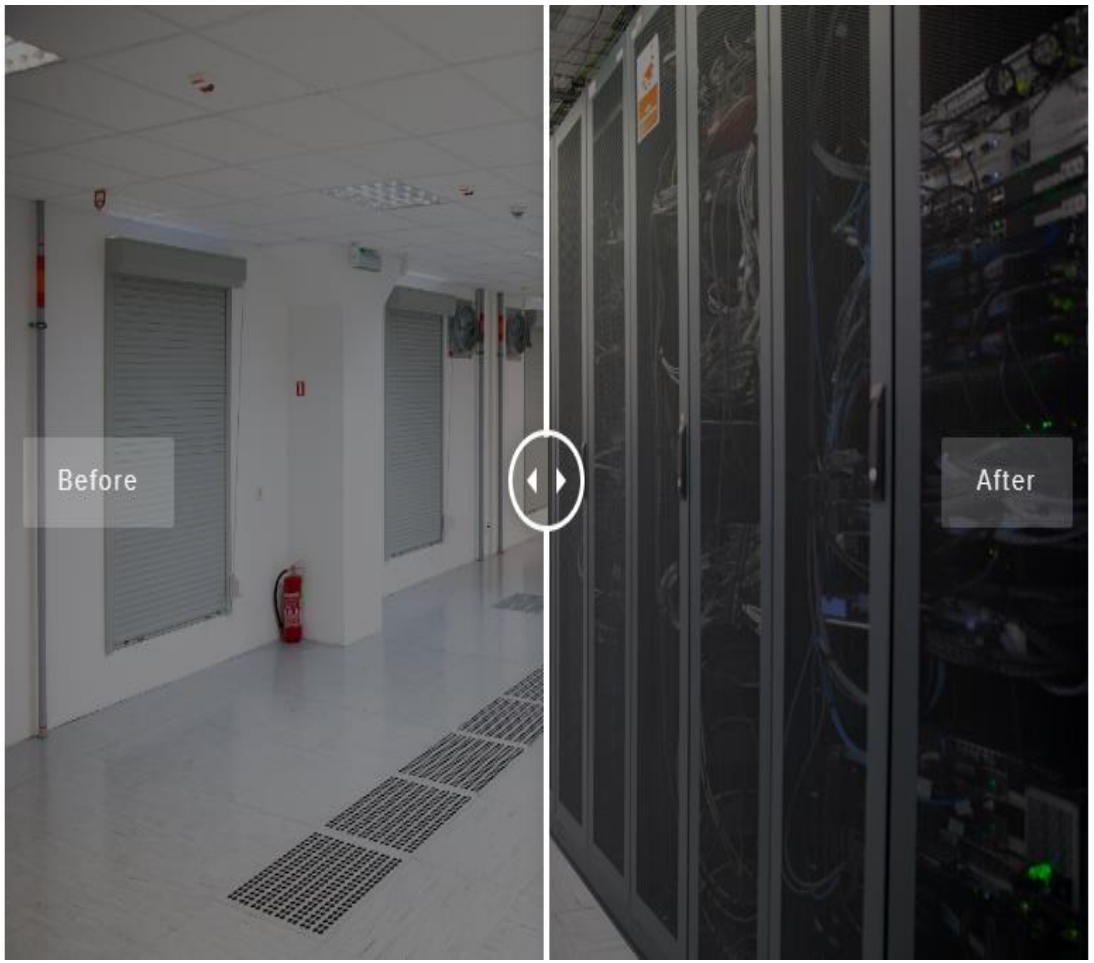
Цистерни з дизпаливом для генераторів / Фото Tet

Кондиціонування

Оскільки перегрів обладнання неприпустимий, а будь-яка обчислювальна система споживає багато енергії і виділяє велику кількість тепла, приміщення машинного залу має дуже добре охолоджуватися. Для охолодження ЦОД використовують професійні прецизійні кондиціонери, а також різні сучасні системи, такі як фрікулінг.

Серверне приміщення дата-центру Dattum розміщується за принципом "кімната в кімнаті", а подвійна підлога розташована на висоті 90 сантиметрів. Усе герметично та надійно.

всередині дата-центру, саме там де розташовані серверні стійки, все повинно бути максимально чисто, тож система кондиціонування та очищення повітря дбає і про чистоту, а на вході в об'єкт, у випадку з Dattum, є автомат для одягання бахіл та спеціальна клейка стрічка на підлозі, яка затримує пил.



Безпека

Обладнання дата-центру має бути захищене від сторонніх осіб. Не менш важливе завдання – забезпечення конфіденційності даних, які зберігаються у центрі обробки даних. У більшості випадків системи безпеки ЦОД включають систему контролю доступу, відеоспостереження, пожежну сигналізацію, протипожежну систему та інші системи. Доступ до обладнання жорстко регулюється, завжди є охорона, а доступ до дата-центру забезпечує система подвійної аутентифікації.

Одним із найважливіших аспектів безпеки дата-центру є протипожежна безпека об'єкта. ЦОД повинен бути максимально захищений у випадку пожежі. Дата-центр Dattum використовує автоматичну систему пожежогасіння – низка датчиків трьох видів (загальна кількість 2000 штук в усьому об'єкті) у будь-який момент готові зреагувати на небезпеку. Крім того, усі системи дублюються, аби виключити помилкові спрацьовування.

Для гасіння пожежі використовується безпечний для здоров'я людини інертний газ IG-55, який у спеціальних балонах постійно підключений до системи. У приміщенні також зберігається додаткова кількість балонів для перезаправки. Система регулярно тестується – фахівці перевіряють датчики та роботу механізмів аби впевнитися у тому, що у потрібний момент об'єкт буде максимально захищений.

Система пожежогасіння у дата-центрі Dattum / Фото Тет

Передача даних

Стабільний і безперебійний процес передачі даних важливий для будь-якого дата-центру. Для його забезпечення використовують як виділені канали, так і загальнодоступні інтернет-мережі з широкою смугою пропускання. Канали обов'язково резервуються.

Диспетчеризація

Забезпечення стабільної роботи всього ЦОД неможливо без системи моніторингу та диспетчеризації. За всіма системами ведеться цілодобове спостереження, а усунення виявлених проблем відбувається по заздалегідь розроблених алгоритмах. Це виключає помилки та дозволяє розв'язувати проблеми максимально швидко.

Рівні центру обробки даних

Рівні центрів обробки даних — це стандартизована система рейтингу, яка вказує на надійність і продуктивність інфраструктури центру обробки даних. Класифікація класифікує об’єкти від Tier I до Tier IV, де Tier I є найменш надійним, а Tier IV – найнадійнішим і відмовостійким.

Рівень I

Центри обробки даних Tier I є найпростішими та найменш надійними об’єктами. Вони мають єдиний шлях живлення та охолодження, що означає, що будь-яке технічне обслуговування або збій призведе до простою. Центри обробки даних рівня I пропонують обмежений захист від фізичних подій і не мають надлишкових компонентів.

Рівень II

Центри обробки даних Tier II мають резервну ємність компонентної інфраструктури сайту, що означає, що вони пропонують покращений захист від фізичних подій. У них є кілька шляхів живлення та охолодження, але вони все ще мають одну точку відмови. Центри обробки даних Tier II надійніші, ніж Tier I, але все ще мають значний ризик простою.

Рівень III

Центри обробки даних Tier III мають кілька шляхів живлення та охолодження, а також мають резервні компоненти, що означає, що вони не мають єдиних точок відмови. Центри обробки даних Tier III пропонують вищий рівень надійності, ніж Tier II, і мають гарантований час безвідмовної роботи 99.982%. Вони також мають відмовостійку конструкцію та можуть виконувати технічне обслуговування та відключення без будь-яких простоїв.

Рівень IV

Центри обробки даних рівня IV є найскладнішими та мають найбільше резервних компонентів. Вони мають кілька шляхів живлення та охолодження, а також мають резервні системи живлення та охолодження, що означає, що вони не мають єдиних точок відмови. Центри обробки даних Tier IV пропонують найвищий рівень надійності та безвідмовної роботи з гарантованим часом безвідмовної роботи 99.995%. Вони також мають відмовостійку конструкцію та можуть виконувати технічне обслуговування та відключення без будь-яких простоїв.

Компоненти ЦОД можна розділити на дві основні частини:

керуючу, що являє собою набір засобів доставки, обробки й зберігання інформації, призначених для спостереження, контролю й координації функціонування об'єктів, що забезпечують інформаційне обслуговування користувачів;

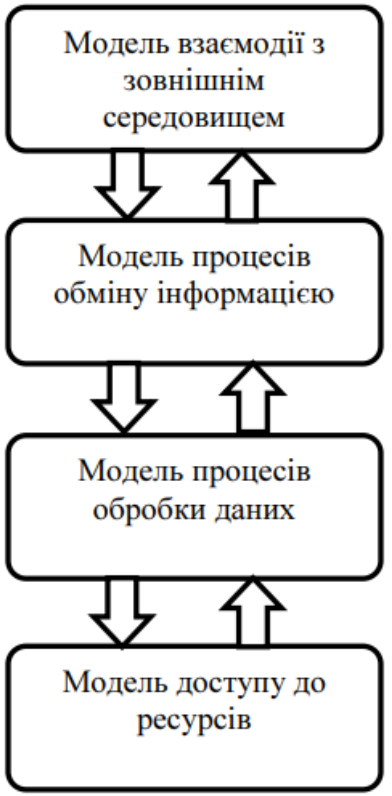
виконавчу систему, що містить ресурси, які використовуються системою керування для надання послуг.

Процес функціонування ЦОД полягає в тому, що під впливом зовнішніх запитів у процесі обробки коригується інформація, що зберігається в базах даних, опитуються, задіюються або звільняються ресурси. Відповідно до задачі у розпорядження користувачів надаються або не надаються необхідні ресурси.

Зазвичай при розробці моделей використовується багаторівнева модель ЦОД. Кожний рівень такої моделі являє собою модель, що характеризує його поведінку на деякому функціональному рівні. При переході від верхніх рівнів до нижніх розкривається принцип побудови ЦОД, а при переході від нижніх до верхніх - розкриваються зміст і призначення ЦОД.

Верхній рівень складають моделі, які описують ЦОД як відкриту систему, що надає послуги за зовнішніми запитами. Аналіз процесів взаємодії ЦОД із зовнішнім оточенням дозволяє одержати комплексні характеристики якості обслуговування користувачів.

Верхній рівень складають моделі, які описують ЦОД як відкриту систему, що надає послуги за зовнішніми запитами. Аналіз процесів взаємодії ЦОД із зовнішнім оточенням дозволяє одержати комплексні характеристики якості обслуговування користувачів. Наступний рівень – моделі обміну інформації, для складання яких необхідно мати інформацію про структуру і функцію програмного забезпечення, способи взаємодії підсистем ЦОД.
Аналіз процесу виконання обміну інформації дозволяє визначити параметри окремих функціональних завдань, реалізованих ЦОД.



Наступний рівень представляє моделі управляючої системи, які на основі інформації про структуру й параметри модулів управління дозволяють визначити функції розподілу часу перебування й імовірності блокування запитів. ЦОД - це система масового обслуговування, оскільки він являє собою безліч апаратних, програмних і інформаційних ресурсів і безліч запитів, що надходять у випадкові моменти часу й конкуруючих за право доступу до цих ресурсів.

Основні критерії якості роботи дата-центру

Роботу конкретного дата-центру прийнято оцінювати за наступними критеріями: аптайм, надійність роботи, відмовостійкість.

Аптайм — це відсоток доступності системи за певний період роботи (наприклад, за добу). Аптайм залежить від багатьох умов — розміру каналу зв'язку і його завантаженості, збоїв в обладнанні, перебоїв з енергопостачанням, перегріву компонентів системи тощо. Для серйозних дата-центрів аптайм становить понад 97%, а в деяких випадках перевищує 99%.

Надійність і відмовостійкість — це можливість дата-центру виконувати свої функції, навіть якщо порушена робота одного або декількох компонентів, або відбулися інші події, наприклад, припинилася подача електроенергії. У дата-центрах домагаються підвищення відмовостійкості за рахунок дублювання кожного елемента — каналів зв'язку, накопичувачів даних, джерел безперебійного живлення, запасних серверів з автоматичним перемиканням в разі виникнення проблем.