**Лекція 2\_ Еталонна архітектура хмарних обчислень**

**(Cloud Computing Reference Architecture)**

**1. Мета**

Мета полягає у визначенні нейтральної референтної архітектури (reference archtecture), що відповідає визначенню хмарних обчислень NIST - NIST Definition of Cloud Computing, яка:

***а) Представляє:***

* три сервісних моделі (Програмне забезпечення як послуга -Software as a Service (SaaS) / Платформа як послуга - Platform as a service (PaaS) / Інфраструктура як послуга - Infrastructure as a Service (IaaS)),
* четыре модели развертывания (*частное облако - private cloud/общее облако - community cloud/публичное облако - public cloud/ гибридное облако - hybrid cloud*) и
* пять основных характеристик (*on-demand self-service/broad network access/resource pooling/rapid elasticity/measured service*)

• Зв'язує різні хмарні сервіси і відображає їх на загальну модель

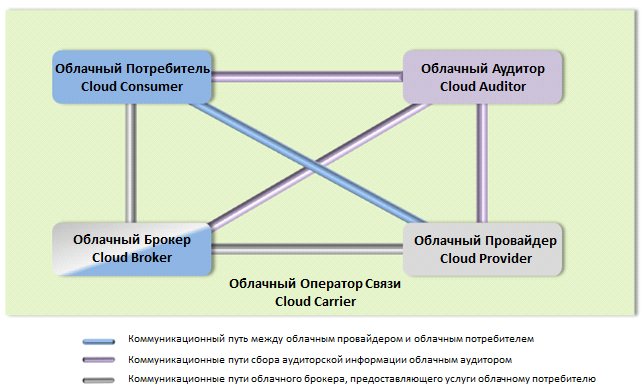
 • Діє як дорожня карта (роадмеп) індустрії ІТ для розуміння, вибору, проектування та / або розгортання хмарної інфраструктури

**2. Референтна архітектура хмарних обчислень - високорівневої погляд**

Референтна архітектура хмарних обчислень NIST містить п'ять головних діючих суб'єктів - акторів (actors). Кожен актор виступает в ролі (role) і виконує дії (activities) і функції (functions). Референтна архітектура представлена ​​як послідовні діаграми зі зростаючою рівнем деталізації.

Серед представлених п'яти акторів, хмарний брокер (cloud broker) - опціональний, тому що хмарні споживачі (cloud consumers) можуть отримувати послуги безпосередньо від хмарного провайдера (cloud provider).

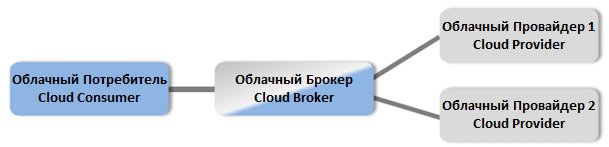
|  |  |
| --- | --- |
| **Актор** | **Визначення** |
| Хмарний Споживач  Cloud Consumer | Особа або організація, що підтримує бізнес-відносини і використовує послуги Хмарних Провайдерів. |
| Хмарний Провайдер  Cloud Provider | Особа, організація або сутність, що відповідає за доступність хмарної послуги для Хмарних Споживачів. |
| Хмарний Аудитор  Cloud Auditor | Учасник, який може виконує незалежну оцінку (assessment) хмарних послуг, обслуговування інформаційних систем, продуктивності і безпеки реалізації хмари. |
| Хмарний Брокер  Cloud Broker | Сутність, керуюча використанням, продуктивністю і наданням хмарних послуг, а також встановлює відносини між хмарність Провайдерами і хмарність Споживачами. |
| Хмарний Оператор Зв'язки  Cloud Carrier | Посередник, який надає послуги підключення та транспорт (послуги зв'язку) <доставки> хмарних послуг від Хмарних Провайдерів до хмарність Споживачам. |



*Взаємодія між акторами в хмарних обчисленнях*

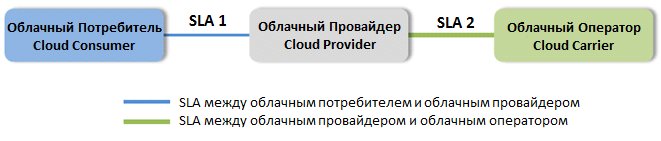
**3. Приклади сценаріїв використання**

**Сценарій 1:** Хмарний споживач може запросити послугу (сервіс) у хмарного брокера замість прямого контактування з хмарним провайдером. Хмарний брокер може створити новий сервіс, комбінуючи набір сервісів або розширюючи існуючий сервіс. У цьому прикладі хмарний провайдер невидимий хмарного споживачеві.



*Сценарій 1 - участь хмарного брокера у взаємодії споживача з провайдером*

Сценарій 2: Хмарний оператор зв'язку предоставлет послуги підключення та транспорт <доставки> хмарних послуг від хмарного провайдера хмарного споживачеві. Хмарний провайдер встановлює угоду про рівень обслуговування SLA з хмарним оператором і може запитувати виділені і захищені з'єднання.



*Сценарій 2 - участь хмарного оператора в наданні провайдером послуг*

Сценарій 3: Хмарний аудитор проводить незалежну оцінку обслуговування і безпеки реалізації хмарної послуги.



*Сценарій 3 - участь хмарного аудитора в оцінці надання провайдером послуг*

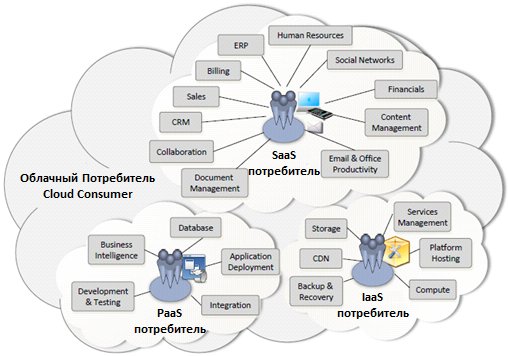
**4. Актори, їх ролі та функції**

Хмарний Споживач

*Особа або організація, що підтримує бізнес-відносини і використовує послуги Хмарних Провайдерів.*

Хмарні споживачі категоризируются за трьома групами, заснованим на їх додатках / різних сценаріях використання.

|  |  |  |
| --- | --- | --- |
| **Тип Споживача** | **Основна діяльність (активності)** | **Приклади користувачів** |
| SaaS | Використовує додатки / сервіси для автоматизації бізнес-процесів | Бізнес-користувачі, адміністратори додатків |
| PaaS | Розробляє, тестує, розгортає і управляє програмами, розгорнутими в хмарному оточенні | Розробники додатків, тестувальники, адмінісратори |
| IaaS | Створює / встановлює, управляє і моніторить сервіси для управління ІТ-інфраструктурою | Системні розробники, адміністратори, ІТ-менеджери |



*Приклади сервісів, доступних хмарним споживачам*

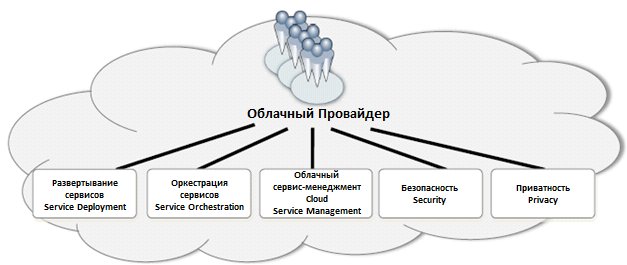
Хмарний Провайдер

*Особа, організація або сутність, що відповідає за доступність хмарної послуги для Хмарних Споживачів.*

Хмарні провайдери виконують різні завдання в різних сервісних моделях.

|  |  |
| --- | --- |
| **Тип Провайдера** | **Основная деятельность (активности)** |
| SaaS | Встановлює, управляє, супроводжує і підтримує програмне забезпечення <розгорнуте> на хмарної інфраструктурі. |
| PaaS | Надає і управляє хмарної інфраструктурою і сполучною програмним забезпеченням (middleware) платформи для споживачів; надає інструменти розробки, розгортання і адмітністрірованія споживачам платформи. |
| IaaS | Надає і управляє фізичними обчислювальними потужностями (processing), системами зберігання, мережами і хостинг-оточенням, а також хмарної інфраструктури для IaaS-споживачів. |

Діяльність хмарних провайдерів обговорюється більш детально з точок зору (в архітектурних перспективи) розгортання сервісів (service deployment), оркестрації сервісів (service orchestration), хмарного сервіс-менеджменту (cloud service-management), безпеки (security) і приватності (privacy).



*Діяльність хмарних провайдерів обговорюється більш детально з точок Хмарний Провайдер - високорівнева погляд*

**Розгортання сервісів (Service Deployment)**

Хмарна система може функціонувати в одній з чотирьох моделей:

* Приватне хмара (Private cloud): Хмарна інфраструктура функціонує цілком з метою обслуговування однієї організації. Інфраструктура може управлятися самою організацією або третьою стороною і може існувати як на стороні споживача (on premise) так і у зовнішнього провайдера (off premise).

* Хмара спільноти або загальне хмара (Community cloud): Хмарна інфраструктура використовується спільно декількома організаціями та підтримує обмежене співтовариство, що розділяють загальні принципи (наприклад, місію, вимоги до безпеки, політики, вимоги до відповідності <регламентам і керівними документами>). Така хмарна інфраструктура може управлятися управлятися самими організаціями або третьою стороною і може існувати як на стороні споживача (on premise) так і у зовнішнього провайдера (off premise).

* Публічне хмара (Public cloud): Хмарна інфраструктура створена в якості загальнодоступної або доступною для великої групи споживачів <не пов'язаної загальними інтересами, але, наприклад, належать до однієї області діяльності>. Така інфраструктура знаходиться у володінні організації, що продає відповідні хмарні послуги / надає хмарні сервіси.

* Гібридне хмара (Hybrid cloud): Хмарна інфраструктура є композицією (поєднанням) двох і більше хмар (приватних, загальних або публічних), що залишаються унікальними сутностями, але об'єднаними разом стандартизованими або пропрієтарними технологіями, що забезпечують портіруемость даних і додатків <між такими хмарами> ( наприклад, такими технологіями, як пакетна передача <даних> для балансу завантаження між хмарами).

**Оркестрації сервісів (Service Orchestration)** передбачає звернення до неї для систематизації, координації і управління хмарної інфраструктурою, призначеної для надання різних хмарних послуг, що забезпечують узгодження бізнес-та ІТ-вимог.

Узагальнена хмарна середовище містить три концептуальних рівня:

* ***Рівень Сервісу (Service Layer):*** Визначає базові сервіси, що надаються хмарним провайдером.

○ SaaS: розгортаються додатки припускають роботу з ними за допомогою звернення до хмари з <спеціально призначених> програмних клієнтів і інших програм, орієнтованих на кінцевих користувачів.

PaaS: Сервіси для споживачів, призначені для розробки і розгортання додатків на хмарної інфраструктурі, що включають контейнери додатків, інструменти розробки додатків, системи управління базами даних і т.п

○ IaaS: Надання обчислювальних потужностей, систем зберігання, мережевих і інших фундаментальних обчислювальних ресурсів, поверх яких хмарні споживачі можуть розгортати та запускати програми на хмарної інфраструктурі.

* ***Рівень Абстракції і Контролю ресурсів (Resource Abstraction and Control Level):***

○ Призначає / надає елементи програмного забезпечення, такі як гипервизор, віртуальні сховища даних і підтримують програмні компоненти, що використовуються для реалізації хмарної інфраструктури, поверх якої може бути визначений / встановлений хмарний сервіс. Також призначає / надає асоційовані функціональні модулі, які керують абстрагованими <таким чином> ресурсами для забезпечення ефективного, безпечного і надійного використання.

* *Незважаючи на те, що на цьому рівні широко застосовується технологія віртуальних машин, не виключаються й інші значення <поняття> необхідної абстракції програмного забезпечення. Цей рівень забезпечує "готовність до хмари" ("cloud readiness"), яка визначається п'ятьма характеристиками, представленими в "Визначенні хмарних обчислень", розробленому NIST.*

* ***Рівень Фізичних Ресурсів (Physical Resource Level): Включає всі фізичні ресурси.***

○ Комп'ютерне обладнання (Hardware): Комп'ютери (CPU, пам'ять), мережі (роутери, мережеві екрани, свічі, мережеві канали та інтерфейси), компоненти зберігання (жорсткі диски) та інші фізичні елементи обчислювальної інфраструктури.

Інженерну інфраструктуру (Facilities): системи кондиціонування (HVAC), харчування, комунікацій та інші елементи фізичної майданчики розгортання комп'ютерного обладнання.



*Оркестрації сервісів хмарних провайдером*

***Хмарний Сервіс-Менеджмент (Cloud Service Management)*** включає всі пов'язані з сервісом функції, необхідні для управління і функціонування сервісів, необхідних або пропонованих хмарним споживачам.

Хмарний провайдер виконує ці функції для підтримки управління хмарними сервісами:

* • Підтримку Бізнесу (Business Support)
* • провіженінг / Конфігурація (Provisioning / Configuration)
* • портіруемость / Інтероперабельність (Portability / Interoperability)



***• Підтримка Бізнесу (Business Support):*** Призначає / надає набір сервісів, пов'язаних з бізнесом і орієнтованих на роботу з клієнтами і підтримують процесами, такими як розміщення замовлень, обробку рахунків і збір платежів. Також включає компоненти, що використовуються для виконання бізнес-операцій, видимих ​​<бізнес-> клієнтам.

* Управління замовниками (Customer Management): керування обліковими записами користувачів, відкриття / закриття / припинення дії облікових записів, управління профілями користувачів, управління взаємодією з замовниками (customer relationship) на основі надання контактів і вирішення питань і проблем замовників, і т.п.

* ○ Управління Контрактами (Contract Management): управління сервісними контрактами, висновок / закриття / припинення дії контрактів, і т.п.

* ○ Управління Постачанням (Inventory Management): настройка і управління каталогом послуг, і т.п.

* ○ Бухгалтерія і Нарахування (Accounting and Billing): управління платіжною інформацією щодо замовників, відправка рахунків на оплату, обробка отримання платежів, відстеження рахунків, і т.п.

* Звітність та Аудит (Reporting and Audit): моніторинг дій користувачів, генерація звітів, і т.п.

* *Ценообразование и Тарификация (Pricing and Rating)*: оценка облачных услуг и определение цен, обработка специальных предложений и правил ценообразования, основанных на профиле пользователя, и т.п.
* ***Провиженинг/Конфигурирование (Provisioning/Configuration):*** включает все связанные с сервисом функции, необходимые для управления и функционирования сервисов, необходимых или предлагаемых облачным потребителям.  
  + *Быстрый провиженинг (Rapid Provisioning):* автоматическое развертывание облачных систем на основе запросов сервисов/ресурсов/возможностей.

○ Модифікація ресурсів (Resource Change): налаштування конфігурацій / призначення ресурсів для відновлення, апгрейда і підключення нових вузлів в хмару.

○ Моніторинг та звітність (Monitoring and Reporting): виявлення та моніторинг віртуальних ресурсів, моніторинг функціонування (дій та подій) хмари і генерація звітів про продуктивність.

○ Вимірювання <показників> (Metering): надання можливостей кількісних вимірів на рівні абстракції, відповідному типу сервісу (наприклад, засобів зберігання, обробки, пропускної спроможності і активних облікових записів користувачів).

○ Управління рівнем обслуговування (SLA Management): визначення параметрів SLA контракту (схема з параметрами якості сервісу - QoS), моніторинг <виконання> SLA, застосування SLA відповідно до заданих політиками.

• ***портіруемость / Інтероперабельність (Portability / Interoperability):***

○ портіруемость:

1. можливість перенесення даних з однієї системи в іншу без необхідності повторного створення або введення описів даних або значну модифікацію переносите додатків.

2. можливості програмного забезпечення або системи виконуватися на більш ніж одному типі або потужності комп'ютера під більш ніж однією операційною системою.

○ Інтероперабельність: можливість взаємодіяти, виконувати програми або передавати дані між різними функціональними одиницями відповідно до заданих умов.

Хмарні провайдери повинні надавати механізми для:

* портіруемость даних (Data Portability)
* Копіювання даних "з" / "в" (Copy data to-from): копіювання даних з / в хмару
* Пакетний перенесення даних (Bulk data transfer): використання диска для пакетного перенесення

* інтероперабельності сервісів (Service Interoperability): дозволяє хмарним споживачам використовувати їх дані і сервіси через у безлічі хмарних провайдерів, використовуючи уніфіковані і розширені інтерфейси управління.
* портіруемость систем (System Portability)

□ Перенесення образів віртуальних машин (VM images migration): міграція повністю зупиненого примірника або образу віртуальної машини від одного провайдера до іншого.

□ Міграція додатків / сервісів (Application / Service migration): міграція додатки / сервісу або поточного утримання від одного сервіс-провайдера до іншого.

**Безпека (Security)**

* Аутентифікація і Авторизація (Authentication and Authorization): аутентифікація і авторизація хмарних споживачів з використанням попередньо створеного мандата доступу.
* Доступність (Availability): налаштування конфігурацій / призначення ресурсів для відновлення, апгрейда і підключення нових вузлів в хмару.

* Конфіденційність (Confidentiality): виявлення та моніторинг віртуальних ресурсів, моніторинг функціонування (дій та подій) хмари і генерація звітів про продуктивність

* *Управление идентификацией (Identity management)*: предоставление возможностей количественных измерений на уровне абстракции, соответствующем типу сервиса (например, средств хранения, обработки, пропускной способности и активных учетныъх записей пользователей).
* *Мониторинг безопасности и обработка инцидентов (Security monitoring & Incident Response)*: определение параметров SLA контракта (схема с параметрами качества сервиса – QoS), мониторинг <выполнения> SLA, применение SLA в соответствии с заданными политиками.
* *Управление политиками безопасности (Security policy management):* генерация/ применение/ аудит/ обновление политик безопасности  для пользователей, получающих доступ к облакам.

***Конфіденційність - захист приватності (Privacy)***

• Захищає достовірні, належні <за призначенням> і відповідні <політикам і правилам> збір, обробку, передачу, використання і зберігання в хмарі персональних даних та інформації, що дозволяє ідентифікувати особу.

**Хмарний Аудитор (Cloud Cloud Auditor)**

*Учасник, який може виконує незалежну оцінку (assessment) хмарних послуг, обслуговування інформаційних систем, продуктивності і безпеки реалізації хмари.*

Хмарний аудитор може давати оцінку сервісів, що надаються хмарним провайдером, в термінах *контролю безпеки (security control), дотримання приватності (privacy impact), продуктивності (performance), і т.п*.

Для аудиту безпеки хмарний аудитор може проводити оцінку контролю безпеки інформаційної системи для визначення меж, для яких контроль виконується відповідним чином, в яких система функціонує за призначенням і виробляють бажаний результат відповідно до вимог безпеки, пред'являти до системи.

**Хмарний Брокер (Cloud Broker)**

Сутність, керуюча використанням, продуктивністю і наданням хмарних послуг, а також встановлює відносини між хмарність Провайдерами і хмарність Споживачами.

У міру еволюції хмарних обчислень, інтеграція хмарних сервісів може виявитися для хмарних споживачів занадто складною для управління.

Основні послуги, що надаються хмарним брокером, включають:

* Сервісне посередництво (Service Intermediation): хмарний брокер розширює заданий сервіс, покращуючи його окремі можливості, і надаючи додаткові сервіси хмарним споживачам.
* Агрегування сервісів (Service Aggregation): хмарний брокер комбінує і інтегрує сервіси в один і більше сервісів. Брокер буде забезпечувати інтеграцію даних і їх безпечний перенесення між хмарним споживачем і хмарними провайдерами.
* Арбітраж сервісів \* (Service Arbitrage): арбітраж сервісів аналогічний агрегування сервісів, але відрізняється тим, що агрегіруемий сервіси не модифікуються. Арбітраж сервісів забезпечує хмарного брокеру гнучкий і вигідний вибір <сервісів>. Наприклад, хмарний брокер може використовувати скоринговий сервіс і формувати найкращий портфель <сервісів для пропозиції хмарним споживачам>.

*\* Аналогічно поняттю арбітражу цінних паперів*

**Хмарний Оператор Зв'язки (Cloud Carrier)**

Посередник, який надає послуги підключення та транспорт (послуги зв'язку) <доставки> хмарних послуг від Хмарних Провайдерів до хмарність Споживачам.

• Надає хмарним споживачам доступ <до хмарним послуг> через мережеві, телекомунікаційні та інші пристрої доступу.

○ Приклад: пристрої мережевого доступу включають комп'ютери, ноутбуки, мобільні телефони, мобільні пристрої доступу в Інтернет (mobile internet devices - MID) і т.п.

Забезпечує доставку <послуг та пристроїв> може забезпечуватися мережевими і телекомунікаційними операторами, а також транспортними агентами.

* *Транспортный агент (transport agent):* бизнес-организация, обеспечивающая физическую транспортировку средств хранения <информации> (storage media), таких как жесткие диски повышенной емкости.

Облачный провайдер должен заключать с облачным оператором связи *соглашение об уровне обслуживания (SLA)* для обеспечения соответствующего уровня сервиса. В общем случае, к облачному оператору связи могут предъявляться требования по предоставлению выделенного и защищенного соединения.



*Комбінована концептуальна діаграма референтної архітектури хмарних обчислень*