**Лекция \_3\_ Хмарні обчислення: огляд і рекомендації**

**Загальне середовище хмарних обчислень** (Розділ 4)

*Рекомендації Національного Інституту Стандартів і Технологій (США)* Special Publication 800-146 (Draft)

 Необхідно розуміти, що термін "хмарні обчислення" охоплює велике різноманіття як систем і технологій, так і моделей розгортання, <надання> послуг і ведення бізнесу.

Ряд тверджень, які іноді робляться щодо хмарних обчислень, наприклад, що вони "масштабируются" або що вони конвертують капітальні витрати (CAPEX) в операційні (OPEX), є вірними тільки для певних видів хмарних систем.

Мета цього розділу полягає в тому, щоб чітко описати поділ систем хмарних обчислень або хмарних систем на п'ять значущих сценаріїв і, для кожного з цих сценаріїв, пояснити основні аспекти (такі, як масштабованість), що вимагають уваги або викликають суперечки, і як ці аспекти адресуються щодо кожного з сценаріїв (2).

2) Цей розділ представляє фізичний - мережевий погляд на те, як передплатники (хмарні споживачі - замовники) сервісів підключені до хмарним системам. Розуміння хмарного і складових частин традиційного "стека" програмного забезпечення, доступних для передплатників є не менш важливим і розглядається в розділах 5, 6 і 7 цього (оригінального) документа.

Як це передбачається у визначенні хмарних обчислень NIST, хмарна система є колекцією ресурсів, доступних через мережу для замовників (тобто хмарних передплатників - хмарних споживачів). У загальному випадку, хмарна система і її передплатники застосовують модель клієнт-сервер, яка передбачає, що передплатники відправляють по мережі повідомлення серверним комп'ютерів, які у відповідь на отримані повідомлення виконують відповідну роботу.



Малюнок 1: Загальний погляд на хмару і передплатників

Малюнок 1 дає загальний погляд на хмару і його клієнтів: хмарні обчислювальні ресурси описані як комплекс взаємопов'язаних \* комп'ютерних систем, доступ до яких клієнти здійснюють по мережі. Як показано на малюнку, можуть з'являтися нові клієнти, старі клієнти можуть йти, в різні моменти часу кількість клієнтів буде різним.

Подібним чином і хмара підтримує пул апаратного забезпечення, яким керує для максимізації (збільшення продуктивності і рівня) сервісу та мінімізації витрат. Для підтримки високої доступності сервісів, незважаючи на очікувані відмови і витікання терміну життя компонент, хмара міру виникнення необхідності \*\* підключає нові і виводить з експлуатації старі або відмовили апаратні компоненти. Хмара ефективно управляє пулом апаратних ресурсів для оптимального, з т.з. витрат, надання сервісів.

Одна зі стратегій <такого управління> полягає в тому, що хмарний провайдер відключає невикористовувані компоненти на період скорочення потреб передплатників. З позицій чи управління споживаної потужністю або поновлення апаратного забезпечення, міграція робочих навантажень (workloads) замовників з одного фізичного комп'ютера на інший є ключовою стратегією, що дозволяє провайдеру оновлювати апаратне забезпечення і консолідувати робочі навантаження без заподіяння незручностей передплатникам.

\*) В даному випадку, grid представляється логічним перевести саме так, тому що хмарні обчислення не завжди припускають використання Grid-технологій. Lingvo Computers дає такі визначення:

• Grid - архітектура, концепція, технологія Grid - орієнтований на віртуалізацію обчислень спосіб організації обчислювального процесу, коли частини завдання розподіляються по всім вільним ресурсам мережі.

• "Grid computing - мережеві (колективні, паралельні, розподілені) обчислення," решітки "обчислювальних ресурсів, grid -Обчислення - термін відноситься переважно до архітектури глобальних, регіональних і відомчих комп'ютерних мереж, передбачає використання вільних в даний момент ресурсів мережі при вирішенні завдань, занадто складних для окремо взятого комп'ютера, і вимагає спеціального ПО.

У свою чергу, хмарні технології безпосередньо не мають на увазі (хоча і не заперечують) використання розподілу виконання частин завдання за різними вузлів "решітки", що представляє собою розподілені обчислювальні ресурси, пов'язані особливим чином для виконання, фактично, масово-паралельних обчислень.

\*\*) напевно, ви звернули увагу, що в пропонованих перекладах "as needed" і "on demand" переводяться не «на вимогу», а «за потребою".

Такий вибір обумовлений більш м'яким і, певною мірою, превентивним для ряду випадків сенсом "в разі потреби". Вимога споживача, яке надійшло в тій чи іншій формі, може не завжди відповідати узгодженим рівнем сервісу (SLA), а необхідність може бути ідентифікована провайдером сервісу взагалі без повідомлення про це клієнта.

 Наприклад, необхідність або потреба виявляється на основі аналізу статистики використання пулу ресурсів клієнтами і прогнозу на подальше зростання утилізації ресурсів, пов'язаний як зі збільшенням потреб існуючих клієнтів в ресурсах, так і зі збільшенням числа клієнтів (екстенсивне або кількісне розвиток) і / або розширенням портфеля наданих послуг того чи іншого типу (інтенсивне або якісний розвиток).

Малюнок 1 представляє лише невелику частину загальних тверджень (міркувань, аспектів), характерних для хмарних обчислень.

Організації припускають, що використання хмарних обчислень має відображати такі загальні положення (представлені нижче). У той же час, багато з тверджень, сформульовані щодо хмарних обчислень (наприклад, що хмари можуть масштабуватися для дуже великих робочих навантажень або їх застосування дозволяє замінювати капітальні витрати операційними), є коректними тільки для певних типів хмар.

Для уникнення плутанини, цей документ явно кваліфікує кожне з таких положень для кожного типу хмари, де таке положення застосовується - тобто кожне твердження має межами <застосовності> змісту ("scope").

Такі кордону, які використовуються в документі, представлені в Таблиці 1.

Таблиця 1: Сценарії - варіанти меж застосування тверджень, які зберігаються відносно хмар (Scope Modifiers for Statements Asserted About Clouds)

|  |  |
| --- | --- |
| **Межі застосування - сценарії** | Опис меж застосування |
| загальний випадок,тобто всі варіанти хмар(General) | Застосовується для всіх моделей розгортання хмар |
| власне приватне хмара(On-site-private) | Застосовується до приватних хмар, реалізованим на майданчику замовника (тобто повністю контрольовані замовником) |
| приватна хмара на аутсоурсінге(Oursourced-private) | Застосовується до приватних хмар, розміщеним на зовнішньому хостингу, яка обслуговується аутсоурсінговой компанією |
| власне хмара спільноти(On-site-community) | Застосовується до хмар спільнот, реалізованим на майданчику замовників, складових співтовариство |
| хмара спільноти на аутсоурсінге(Outsourced-community) | Застосовується до хмар спільнот, чиї сервери (і інше апаратне забезпечення - наприклад, системи зберігання) розміщені на зовнішньому хостингу, яка обслуговується аутсоурсінговой компанією |
| публічне хмара(Public) | Застосовується до публічних хмарах |

Нижче розглядається кожен з представлених сценаріїв меж застосування.

Наступні твердження є загальними по своїх кордонів застосовності, тобто коректні незалежно від моделі розгортання або сервісної моделі (тобто моделі надання послуг):

* ***Залежність від мережі (Network dependency) - загальний випадок.*** Передплатники, будучи клієнтами (з т.з. бізнесу), потребують працюючому і захищеному сервері доступі до хмари. Якщо мережа ненадійна (reliable у всіх сенсах - стійкості доступу і захищеності), хмара не буде вважатися надійним з точки зору передплатника.
* ***Передплатники повинні володіти навичками в ІТ (Subscribers still need IT skills) - загальний випадок***. Експлуатуючи <на своєму майданчику> серверні комп'ютери, провайдер може зменшити потребу організацій-передплатників в ІТ-персонал. Однак, передплатники будуть здійснювати доступ в хмару з своїх клієнтських систем, що вимагають управління, супроводу, підтримки, забезпечення безпеки тощо
* ***Місце виконання робочих навантажень призначається динамічно і приховано від клієнтів*** (Workload locations are dynamically assigned and are thus hidden from clients) - загальний випадок.

3) У деяких випадках (наприклад, сервісної моделі IaaS, описаної в розділі 7 оригінального документа) робоче навантаження може виконуватися в заданому місці в певний проміжок часу часу перед здійсненням міграції;

в інших випадках (наприклад, сервісної моделі PaaS, описаної в розділі 6 оригінального документа) робоче навантаження може бути спочатку розподіленої сутністю, послідовно виконує операції для передплатників на потенційно різних серверах - при цьому, <оброблювані> дані існують в географічно розподіленому сховищі.

* ***Ризики множинної оренди (Risks from multi-tenancy) - загальний випадок.*** Робочі навантаження різних клієнтів можуть виконуватися одночасно на одних і тих же хмарних системах і локальної мережі, будучи розділеними тільки за допомогою політик доступу, визначених на рівні програмного забезпечення провайдера. Уразливості в цьому програмному забезпеченні або в політиках можуть завдати шкоди безпеці передплатників.
* ***Імпорт / експорт даних і обмеження можливості їх виконання*** \* ***(Data import / export, and performance limitations) - загальний випадок.*** В силу того, що передплатники здійснюють доступ <до хмари> по мережі, необхідні часові характеристики пакетного (bulk) імпорту та експорту даних можуть перевищити можливості мережі. Крім того, робота в режимі реального часу або обробка критично важливих запитів можуть виявитися проблематичні через мережевих затримок і інших обмежень.

 \*) Мається на увазі, що мова йде не тільки про обмеження продуктивності, але і інших можливих обмеженнях, що не дозволяють забезпечити необхідні параметри масового введення / виведення даних в / з хмарну систему.

Організації, які розглядають можливість використання хмарних обчислень, повинні брати до уваги ці загальні міркування і їх можливі наслідки для своєї бізнес-моделі і досягнення довгострокових цілей (місії).

Однак, недостатньо приділяти увагу тільки загальним аспектам хмарних обчислень. Хмари також описуються межами застосовності однієї або декількох характеристик, представленими в Таблиці 1. Організації, які обговорюють застосування хмар, повинні детально розглядати аспекти використання різних сценаріїв (варіантів реалізації з урахуванням меж застосування) хмар, які є предметом такого обговорення. Кожна з альтернатив самостійно розглядається нижче в окремому розділі (цього і, ширшого, оригінального) документа, фокусуючись на заданих межах застосовності (4).

4) Цей документ не повторює ті чи інші фрагменти тексту. Однак, для конкретних типів хмар, може бути описано більше міркувань, які є значущими для кожного конкретного типу; в цьому випадку, назва загальної характеристики / затвердження може використовуватися знову, але з поясненням, специфічним для конкретного типу хмари.

**4.1 Розуміння того, хто контролює ресурси в хмарі**

**(Understanding Who Controls Resources in a Cloud)**

Іноді стверджується, що при порівнянні використання хмар з традиційною моделлю "внутрішніх" (on premises) обчислень, хмарна модель вимагає від передплатників передачі провайдеру двох важливих можливостей, які передбачають високий рівень довіри передплатника до провайдера:

* Контролю (Control): можливості вирішувати, хто і що може отримувати доступ до даних і програм передплатника, і виконувати <ті чи інші> дії (такі як стирання даних або відключення від мережі), які повинні бути зроблені, але без додаткових дій, які в свою чергу можуть не відповідати намірам передплатника

 (наприклад, передплатник запитує стирання об'єктів даних, який мав би супроводжуватися неявним їх копіюванням з ініціативи провайдера).

* Видимості - явності дій (Visibility): можливості здійснення моніторингу статусу програм і даних передплатника і того, як до них здійснюється доступ.

Однак, кордони контролю і видимості, які необхідно передати провайдеру з боку передплатників, залежать від багатьох факторів, включаючи фізичне володіння і можливість конфігурації (з високим рівнем довіри) механізмів захисту кордонів доступу до обчислювальних ресурсів передплатників.

Цей документ використовує концепцію кордонів доступу (access boundaries) для структурування і характеристики різних моделей розгортання хмар.

Малюнок 2 ілюструє ключову концепцію комп'ютерної безпеки \*, пов'язану з кордонами і контролем - периметр безпеки (security perimeter).



*Figure 2: Периметр безпеки*

Як показано на малюнку, периметр безпеки виконує роль бар'єру щодо <операцій> доступу: сутність, які знаходяться всередині периметра, можуть виробляти вільний доступ до ресурсів, що знаходяться тільки всередині периметра;

проте, суті, знаходяться за межами периметра, можуть отримувати доступ до ресурсів усередині периметра якщо тільки це дозволено засобами контролю кордонів (контролер кордонів - boundary controller) на основі застосування відповідних політик доступу.

Незважаючи не те, що ці терміни часто використовуються при обговоренні мережевих екранів і мереж, концепція периметра безпеки, в дійсності є більш загальною і може використовуватися, наприклад, для опису меж між різними рівнями привілеїв виконання програмного забезпечення, тобто кордонів <між> додатками і операційною системою.

Саме по собі визначення периметра безпеки НЕ є адекватним механізмом забезпечення безпеки. Однак контроль периметра безпеки є важливим елементом побудови безпечних систем.

**Типові контролери кордонів** включають

* мережеві екрани (firewalls),
* засоби блокування доступу (guards)
* віртуальні приватні мережі (VPN - Virtual Private Networks).

Організація може домогтися оцінки кількісних показників як щодо контролю використання ресурсів, так і моніторингу доступу до них (5).

Більш того, переконфігуріруя периметр безпеки, організація може адаптувати його до мінливих потреб (наприклад, блокування або дозволу протоколів або форматів даних, виходячи із змін бізнес-умов).

5) Коли існують неконтрольовані шляху <доступу> до комп'ютерних ресурсів, периметр безпеки є порушеним (в оригіналі - ослабленим, weakened) або навіть відсутнім.

Поширюються бездротові комунікації, наприклад, є загрозою периметру безпеки, починаючи з того, що не може бути надійного шляху впровадження <контролера кордонів> між зовнішніми і внутрішніми сутностями.

 Аналогічно, багато організацій використовують мобільні пристрої, які іноді підключаються <до ресурсів>, перебуваючи всередині периметра, а іноді залишаються без <належного захисту>, наприклад, під час поїздок.

Різні моделі розгортання хмар, описані в визначенні хмарних обчислень NIST, мають на увазі розміщення контрольованого передплатником периметра безпеки і, отже, рівень контролю, який передплатники можуть здійснювати щодо ресурсів, що довіряють, хмари (тобто переданих під управління провайдера хмари з певним рівнем довіри цього провайдеру).

Визначення хмарних обчислень NIST описує чотири моделі розгортання: приватна хмара (private), хмара спільноти (community), публічне хмара (public), і гібридне хмара (hybrid). Однак, кожна з моделей приватного хмари і хмари спільноти допускають два варіанти - сценарію <розгортання>, які повинні розглядатися окремо, через вплив на периметр безпеки: чи буде він власний (on-site) або на аутсоурсінге (outsourced).

Гібридна модель розгортання є комбінацією інших моделей і, тому, гібридне розгортання може припускати і вплив <на периметр безпеки> його елементів - "будівельних блоків", і унікальні аспекти впливу, що виникають в результаті об'єднання безлічі систем в більш комплексні інтегровані системи.

**4.2 Сценарій власного приватного хмари (The On-site Private Cloud Scenario)**

Малюнок 3 представляє простий погляд на власне приватне хмара (on-site private cloud). Як показано на малюнку, периметр безпеки простягається навколо власних ресурсів передплатника і ресурсів приватного хмари. Приватне хмара може бути централізованим на одному майданчику або розподіленим між декількома майданчиками передплатника.

Периметр безпеки буде існувати тільки в тому випадку, якщо передплатник його реалізує. У разі реалізації, периметр не гарантує контролю всіх ресурсів приватного хмари, але його існування дає передплатнику можливість здійснювати контроль ресурсів, довірених власним приватному хмарі.



*Малюнок 3: Власне приватне хмара*

Незважаючи на те, що загальні припущення залишаються вірними для власного приватного хмари, цей сценарій дозволяє припустити і інші, в т.ч. більш детально описані аспекти, які необхідно прийняти до уваги організаціям, що розглядає використання власних приватних хмар:

***Залежність від мережі (Network dependency) - власне приватне хмара (on-site-private).***

Залежно від конфігурації (наприклад, один фізичний сайт, захищена мережа хмари), залежність від мережі для власного приватного хмари може обмежуватися залежністю від мережевих ресурсів, які контролює передплатник (наприклад, локальна мережа). У цьому сценарії можуть бути виключені такі проблеми мереж великого масштабу (large-scale networks), як "затори" Інтернет або комунікації з віддаленими (в сенсі remote) серверами доменних імен Інтернет (Internet DNS). Крім того, якщо реалізований периметр безпеки для високих рівнів захисту, не у всіх випадках стає необхідним застосування таких механізмів захисту, як багато-факторна аутентифікація і наскрізне шифрування при обміні всередині периметра навіть при досить обережних (мінімізують відповідні ризики) політиках безпеки.

Якщо організація-передплатник має безліч фізичних майданчиків і організовує доступ з різних майданчиків до одного і того ж приватному хмарі, передплатник повинен забезпечити контроль комунікацій між майданчиками, (наприклад, лінії зв'язку з шифруванням) або використовувати криптографічні засоби (наприклад, VPN) поверх менш контрольованих засобів комунікацій, таких як публічний Інтернет.

Обидві ці опції мають ризиками мережевий доступності та безпеки приватного хмари, в силу того, що існує залежність від продуктивності ресурсів (комунікаційних засобів), які перебувають за межами області, контрольованій передплатником, і тому, що будь-які помилки в реалізації і конфігурації криптографічних механізмів можуть дозволити отримати доступ ззовні.

***Передплатники повинні володіти навичками в ІТ (Subscribers still need IT skills) - власне приватне хмара (on-site-private).*** Організації-передплатники будуть потребувати традиційних ІТ-навички, необхідні для управління призначеними для користувача пристроями

з яких здійснюється доступ до приватного хмара, при цьому для них актуальні вимоги щодо наявності навичок і в частині хмарних технологій. Раніше, на етапі розгортання власного приватного хмари, організації-передплатники можуть захотіти паралельно підтримувати протягом певного проміжку часу \* і хмарні і традиційні засоби.

 Крім того, можуть вимагатися нові навички для роботи з хмарами. Наприклад, організаціям, які виконують роботи, що вимагають інтенсивних обчислень, може знадобитися згодом реорганізувати ці роботи таким чином, щоб вони могли використовувати високий рівень паралелізму хмарних ресурсів. Організаціям, що обробляють великі обсяги даних, в свою чергу, може знадобитися розвиток навичок використання хмарних систем зберігання (в загальному сенсі, а не тільки апаратних).

***Місце виконання робочих навантажень призначається динамічно і приховано від клієнтів (Workload locations are hidden from clients) - власне приватне хмара (on-site-private).*** Як і в загальному випадку, приватна хмара, з точки зору управління апаратними ресурсами, має забезпечувати можливість міграції робочих навантажень між машинами <фізичними вузлами> без заподіяння клієнтам будь-яких незручностей, тобто навіть без необхідності клієнтам знати про це. У той же час, в разі власного приватного хмари, організація передплатника вибирає фізичну інфраструктуру для розгортання та експлуатації приватного хмари і, отже, визначає можливе географічне розміщення місця виконання робочих навантажень.

І якщо індивідуальні клієнти можуть не знати, де саме їх робочі навантаження фізично виконуються в даний момент часу в термінах інфраструктури організації передплатника, сама організація має таку знанням і контролем всіх робочих навантажень, яким дозволено виконуватися <у власному приватному хмарі>.

***Ризики множинної оренди (Risks from multi-tenancy) - власне приватне хмара (on-site-private).*** Як і в загальному випадку, робочі навантаження різних клієнтів можуть виконуватися одночасно в тих же системах і мережах, будучи розділеними тільки за допомогою політик доступу, визначених на рівні програмного забезпечення провайдера.

Уразливості в цьому програмному забезпеченні або в політиках можуть завдати шкоди безпеці організації передплатників, роблячи робочі навантаження клієнтів видимими / доступними іншим сторонам, в порушення політик безпеки. Власне приватне хмара <за своєю природою> в якійсь мірі пом'якшує ці ризики, <спочатку> обмежуючи число можливих порушників; зазвичай, всі клієнти є членами організації-передплатника або авторизованими партнерами або гостями (guest в термінах мережевого доступу), однак, власне приватне хмара залишається вразливим до атак, виробленим авторизованими, але мають злий умисел інсайдерами. .

Різні організаційні функції, такі як платіжні відомості, сховища персональних даних або створена інтелектуальна власність, можуть бути схильні до тих же уязвимостям в безпеці, які можуть дозволити надати доступ користувачам, неавторизованих для доступу до певних класів даних, і які можуть розкрити дані <зовні> з власного приватного хмари.

***Імпорт / експорт даних і обмеження можливості їх виконання (Data import / export, and performance limitations) - власне приватне хмара (on-site-private).***

Як і в загальному випадку, необхідні операції пакетного (bulk) імпорту та експорту обмежені пропускною спроможністю мережі, а робота в режимі реального часу або обробка критично важливих запитів можуть виявитися проблематичні, в силу мережевих обмежень (в тому числі, затримок при передачі даних по мережі - network latency). В окремому випадку, якщо у передплатника є тільки одна площадка, якої потрібен доступ до власного приватного хмари, передплатник може бути забезпечений доступом до локальної мережі, що надає вищу продуктивність, ніж та, яка може бути досягнута при доступі через глобальну мережу.

***Потенційно більш сувора захист від зовнішніх загроз (Potentially strong security from external threats) - власне приватне хмара (on-site-private).*** При використанні власного приватного хмари, передплатник має можливість реалізації відповідного <більш> суворого периметра безпеки для захисту ресурсів приватного хмари від зовнішніх загроз, ніж це може бути досягнуто для ресурсів, що не відносяться до хмари. Для не настільки значущих даних (low-impact data - дані, ризик витоку яких може привести лише до незначних наслідків або взагалі не має значення) і їх обробки, периметр безпеки може містити <лише стандартні> набори правил, що визначаються комерційними мережевими екранами і VPN.

Для більш значущих даних, периметр безпеки може створюватися з застосуванням більш строгих обмежують політик мережевих екранів, багатофакторної аутентифікації і навіть його фізичного ізолювання.

***Значні первинні інвестиції в побудову і міграцію хмари (Significant-to-high up-front costs to migrate into the cloud) - власне приватне хмара (on-site-private).*** Власне приватне хмара вимагає установки програмного забезпечення для управління хмарою на обчислювальних системах організації-передплатника.

Якщо планується, що хмара буде підтримувати робочі навантаження, які передбачають інтенсивні обчислення або обробку даних, <відповідне> програмне забезпечення повинно бути встановлено на великій кількості широко-поширених (більш дешевих - commodity) систем або на меншій кількості високопродуктивних (більш дорогих) систем. Установка хмарного програмного забезпечення і управління такою інсталяцією призведе до значних первинним вкладенням (up-front costs), навіть якщо хмарне програмне забезпечення є вільним, і навіть якщо більша частина <планованого до використання в хмарі> обладнання вже існує в організації.