МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ І.С. Скарга-Бандурова
«____»_____ 20__ р.

ДИПЛОМНИЙ ПРОЕКТ (РОБОТА) БАКАЛАВРА

ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

Засоби управління документацією в хмарному сховищі

Освітній рівень"бакалавр"
Спеціальність 123 "Комп'ютерна інженерії"

Науковий керівник роботи: _____ (підпис) Г.Ф.Кривуля (ініціали, прізвище)

Консультант з охорони праці: _____ (підпис) Я.О.Критська (ініціали, прізвище)

Здобувач вищої освіти: _____ (підпис) І.В.Малижко (ініціали, прізвище)

Група: КІ-16з

Сєвєродонецьк 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітній рівень Бакалавр
Спеціальність 123 "Комп'ютерна інженерія"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Т.в.о. завідувача кафедри _____
_____ С.О. Сафонова
«_____» _____20____р.

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) БАКАЛАВРА

Малижко Ігорю Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Засоби управління документацією в хмарному сховищі

керівник проекту (роботи) Кривуля Геннадій Федорович, д.т.н., проф.
(прізвище, м.'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «30» 04 2020 р. № 77/15.15
2. Строк подання студентом роботи 10.06.2020
3. Вихідні дані до роботи Матеріали переддипломної практики, Theoretical Studies, Cloud Technology, Google Drive, Amazon Web Services, Amazon Elastic Compute Cloud EC2

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Вступ до технології хмари, теоретичні дослідження, проектування програмної системи, опис програмного забезпечення, охорона праці, висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Критська Я.О. ст. викл. кафедри КНІ		

7. Дата видачі завдання 30.04.2020

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Розробка технічного завдання	01.05.2020-07.05.2020	
2	Аналіз завдання, огляд літератури	08.05.2020-10.05.2020	
3	Аналіз технічних засобів та розробка алгоритму	10.05.2020-13.05.2020	
4	Розробка частини проекту "Охорона праці"	13.05.2020-15.05.2020	
5	Програмна реалізація	15.05.2020-01.06.2020	
6	Оформлення пояснювальної записки та презентації	2.06.2020-09.06.2020	

Здобувач вищої освіти _____ І.В.Малижко
(підпис) (прізвище та ініціали)

Науковий керівник _____ Г.Ф. Кривуля
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка до дипломної роботи бакалавра: 94 сторінок, 15 фотографій, 7 таблиць, 31 бібліографічне джерело посилань, 1 додаток.

Метою даного дипломного проекту є аналіз концепції Хмари, електронне навчання на базі хмарних обчислень забезпечує безперервне навчання (у будь-який час, в будь-якому місці та на будь-якому пристрої) та спільне навчання. Хмарні обчислення в академічному середовищі, такі як університет, виграють від кожного студента, факультету, адміністратора та дослідника. Більшість університетських інфраструктур недостатньо використовуються, а в деяких випадках надвикористання ресурсів відбувається для того, щоб збалансувати використання ресурсів, які нам потрібні еластичні технології. Для розробки платформи електронного навчання для іноземних студентів комп'ютерних наук та дослідників слід враховувати нові методології для проектного, проблемного навчання та віртуальної комп'ютерної лабораторії. Цей тип хмарного електронного навчання надає нові методики змішаного навчання для освіти. У цьому проекті пропонується академічна хмара, щоб забезпечити нову еру в електронному навчанні. Ця структура стосується послуг та розгортання хмари в новому вимірі, і кожен шар визначає основні компоненти, необхідні для побудови академічної хмари в університеті.

Ключові слова: хмара, сервіс, хмарні технології, хмарні сервіси, хмарні обчислення, модель розгортання, модель обслуговування, провайдер, клієнт.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ....6
ВСТУП....7
1 ВСТУП ДО ТЕХНОЛОГІЇ ХМАРИ....11
1.1 Цілі хмарних обчислень....14
1.2 Архітектура та підходи хмарних обчислень....15
1.3 Проблеми та рішення....20
1.3.1 Хмарні обчислення безпеки....20
1.3.2 Безпека мережі....21
1.3.3 Інтерфейси....22
1.3.4 Безпека данних....22
1.3.5 Віртуалізація....23
1.5.6 Управління....24
1.3.7 Відповідність....25
1.3.8 Складність....26
1.3.9 Стандартизація хмарних обчислень....27
1.3.10 Стандартизація хмари.....27
2 ТЕОРЕТИЧНІ ДОСЛІДЖЕННЯ....29
2.1 Види хмарних обчислень у університетах....31
2.1.1 Публічна хмара....32
2.1.2 Приватна хмара для університетів....33
2.1.3 Гібрид....35
2.1.4 Спільнота....36
2.2 Використання хмарної платформи Amazon Web Services....37
2.2.1 Amazon EC2....37
2.2.2 Amazon VPC....39
3 ПРОЕКТУВАННЯ ПРОГРАМНОЇ СИСТЕМИ....40

3.1 Архітектура системи 44
3.2 Дизайн системи 46
3.3 Хостинг веб-застосунку на Amazon Services 48
3.4 Архітектура системи 49
3.5 Структура системи 52
4 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 55
4.1 Файловий хостинг ownCLoud 55
4.1.1 Реєстрація для AWS 56
4.1.2 Створення користувача IAM 57
4.1.3 Створіть пару ключів 59
4.1.4 Створити віртуальну приватну хмару (VPC) 61
4.1.5 Створити групу безпеки 62
4.2 Огляд архітектури ownCloud 65
4.3 Створення програми ownCloud 65
4.3.1 Конфігурація Apache 65
4.3.2 Доступ до веб-інтерфейсу ownCloud 66
4.3.3 Спільне використання файлів локально 68
4.3.4 Перевірка власного додаткаCloud на веб-сторінці 68
5 ОХОРОНА ПРАЦІ 71
5.1 Аналіз потенційних небезпечних і шкідливих виробничих чинників проектованого об’єкту, що мають вплив на персонал 71
5.2 Заходи щодо техніки безпеки 73
5.3 Заходи, що забезпечують виробничу санітарію і гігієну праці 76
5.4 Рекомендації по пожежній безпеці 80
ВИСНОВКИ 85
СПИСОК ДЖЕРЕЛ ПОСИЛАНЬ 86
ДОДАТОК А КОМП’ЮТЕРНА ПРЕЗЕНТАЦІЯ 90

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface, інтерфейс прикладного програмування

AWS – Amazon Web Services, веб-служби Amazon

GB – Gigabyte, Гігабайт

HTTP – Hypertext Transfer Protocol, протокол передачі гіпертексту

ICT- Information and Communication Technologies, інформаційні та комунікаційні технології

IDE – Integrated Development Environment, інтегроване середовище розробки

IaaS – Infrastructure as a Service, інфраструктура як послуга

IT – Information Technology, інформаційні технології

JSON – JavaScript Object Notation, об'єктне позначення JavaScript

JS – Javascript

JVM – Java virtual machine, віртуальна машина Java

KPMG- Klynveld Peat Marwick Goerdeler (accounting firm), Клинвелд Торф Марвік Гьорделер (бухгалтерська фірма)

MID – Mobile Internet Devices, мобільні Інтернет-пристрої

OSS – Open Source Server, відкритий вихідний сервер

PaaS – Platform as a Service, платформа як послуга

ROI – Return-On-Investment, прибуток-на-інвестиції

SaaS – Software as a Service, програмне забезпечення як послуга

SDK – Software Development Kit, комплект розробки програмного забезпечення

VPN – Virtual Private Network, віртуальна приватна мережа

WS - Web service, веб-сервіс

ВСТУП

При підключенні електричного приладу до розетки, ми не дбаємо про те, як виробляється електрична енергія та як вона потрапляє до цієї розетки. Це можливо тому, що електроенергія віртуалізована; тобто, вона легко доступна з настінної розетки, яка приховує електростанції та величезну розподільчу мережу. Поширюючись на інформаційні технології, ця концепція означає надання корисних функцій, при цьому приховуючи роботу внутрішніх органів. Сама обчислювальна техніка, що вважається повністю віртуалізованою, повинна дозволяти комп'ютерам будувати з розподілених компонентів, таких як обробка, зберігання, дані та програмні ресурси [1]. Такі технології, як кластер, сітка, і тепер хмарні обчислення, спрямовані на те, щоб дозволити доступ до великих обсягів обчислювальної потужності повністю віртуалізованим способом, агрегуючи ресурси і пропонуючи єдиний системний погляд. Крім того, важливою метою цих технологій є постачання комп'ютерів як утиліти. Утиліти обчислень описують бізнес-модель постачання обчислювальної потужності на вимогу; споживачі платять постачальникам на основі використання (“pay-ass-you-go”), подібно до того, як ми в даний час отримуємо послуги від традиційних комунальних послуг, таких як вода, електрика, газ і телефонія. Хмарні обчислення були сприйняті як парасольковий термін для опису категорії складних обчислювальних послуг на вимогу, які спочатку пропонували комерційні провайдери, такі як Amazon, Google і Microsoft. Він позначає модель, на якій обчислювальна інфраструктура розглядається як «хмара», з якої підприємства та особистості звертаються до заявок з будь-якої точки світу [2]. Основним принципом, що стоїть за цією моделлю, є забезпечення обчислень, зберігання та програмного забезпечення «як послуги».

Хмарні обчислення — це еволюція різноманітних технологій, які об'єдналися для зміни підходу організації до побудови IT-інфраструктури. Не існує нічого принципово нового в будь-якій технології, що складають хмарні обчислення, оскільки більшість цих технологій використовувалися вже давно. Термін "хмарні обчислення" описує різні типи обчислювальних концепцій, які включають велику кількість комп'ютерів, підключених через мережу зв'язку в реальному часі (як правило, Інтернет). Хмарні обчислення покладаються на обмін різними ресурсами (наприклад, мережами, серверами, сховищами, додатками та послугами) для досягнення узгодженості та економії масштабу, і надає найбільший інтерес, як максимально підвищити ефективність використання спільних ресурсів. Ця дисертація дає уявлення про концепції та термінології хмарних обчислень. Крім того, вона дасть крок за кроком приклад створення хмари за допомогою технології інфраструктури Amazon EC2 як послуги (IasS). Ключові слова: хмара, хмарні обчислення, Amazon EC2, інфраструктура як послуга (IaaS), веб-служба.

Освіта поступово розширюється, і об'єкт освіти повільно перетворюється на соціальний персонал. Метод навчання від чорної дошки до онлайн зростає швидше, ніж будь-коли. Онлайн-викладач, який допомагає, повинен пройти заняття в будь-яку годину - це розвиток навчання за допомогою технології. Електронне навчання та онлайн-рішення - це те, що нам потрібно в освітньому середовищі. Зі збільшенням кількості отримуючих освіту з'явилася низка нових проблем. Наприклад: Оскільки методи навчання змінюються, існуючі методи навчання та навчання не можуть задовольнити попит; і при постійному розширенні освіти, існуючі навчальні заклади також потребують постійного оновлення. Коли з'являється Cloud Computing, він надає нове рішення для створення уніфікованої, відкритої і гнучкої платформи навчання мережі і зменшення апаратного внеску.

Інтернет — це ресурс, в якому ми можемо трансформувати хмарні обчислення, він може доставляти найсучасніші програмні засоби та навчальні матеріали, апаратні ресурси та послуги для студентів і педагогів навіть у найбідніших або віддалених шкільних округах штату, без необхідності вдосконалених IT-знань у цих місцях. В той же час він робить значно більше, забезпечуючи необхідну допомогу для поточних напружених бюджетів освіти [3]. IT-компанії прагнуть заохотити освітнє впровадження хмарних обчислень; наприклад, Google Apps for Education Suite містить Google Mail, Календар, Обговорення, Документи, Сайти та Відео з нульовою вартістю та без реклами [4], відповідно до аналізу витрат Forrester [9], Служби Google є більш ефективним, ніж Microsoft Exchange електронної пошти. Виходячи з дослідження CSU, витрати на ліцензування програмного забезпечення, серверне обладнання та штатне забезпечення для підтримки 50 000 користувачів за допомогою електронної пошти Microsoft Exchange (кількість облікових записів електронної пошти для студентів на базі CSU) становитимуть $ 9,774,000 на рік [5]. Вартість Служб Google для підприємств становить 50 доларів на одного користувача на рік, або 50 тисяч користувачів - $ 2,500,000 на рік. Однак вартість освітньої версії Служб Google становить $ 0 на рік [5]. Як ми бачимо з цього прикладу, промислове рішення для обчислювальної техніки для освітніх установ вже дало оцінку економії приблизно від $ 9,774,000 на рік до $ 2,500,000 на рік у "версії підприємств" або до нульової вартості ліцензування та обладнання в “освітній версії”. ”. Беручи до уваги два останніх прикладу, ми бачимо, що обидва підходи, промислові (або комерційні) та некомерційні рішення для хмарних обчислень можуть бути успішно використані в навчальних закладах, і інший приклад: IBM запустила IBM Cloud Academy, яка є глобальним форумом для викладачі, дослідники та IT-фахівці з освітньої галузі з метою впровадження ініціатив у сфері хмарних обчислень, розвитку навичок та обміну передовим досвідом для зниження експлуатаційних витрат,

одночасно покращуючи якість та доступ до освіти. Таким чином, користувачам не потрібно купувати сервер, тільки необхідно придбати відповідні "послуги", щоб створити ефективну мережеву платформу для навчання [7]. Використання хмарних обчислень в академіках університетів не усвідомлює переваг і характеристик мінімізації витрат хмарних обчислень. З точки зору управління IT, це радикально знижує витрати на управління ресурсами - включаючи персонал з електроенергії, охолодження та управління системою, одночасно підвищуючи використання серверів і ліцензій на програмне забезпечення, що в свою чергу знижує вимоги до закупівель [6].

Навчання студентів більше не обмежується у класі в епоху електронного навчання 2.0 [8]. Середовище IT-освіти можна покращити, щоб дозволити студентам отримати доступ до навчальних ресурсів у будь-якому місці. Багато відкритих університетів є гарним прикладом електронного навчання, де студенти можуть вивчати і отримувати дійсні сертифікати про завершення кожного предмета. Вільне програмне забезпечення може бути прийняте для побудови служби хмарних обчислень для середовища IT, як OpenOffice.org, таких як обробка текстів, електронні таблиці та презентації. Для підключення до служби хмарних обчислень для навчання потрібний лише браузер.

Утримання десятків комп'ютерів в лабораторіях стає тягарем для системного адміністратора. Саме тому в дипломній роботі була запропонована бездискова кластерна обчислювальна середовище в комп'ютерному класі і розробка навчальної системи управління мережею. У цьому дипломі ми обговорюємо парадигму та характеристики «хмарних обчислень», моделі обслуговування та розгортання, реалізації хмарних сервісів у університетах, а також різні можливості та переваги Cloud Computing для університетів та академічних установ. Нарешті, ми пропонуємо прототип дизайну Cloud Computing для академічного середовища.

1 ВСТУП ДО ТЕХНОЛОГІЇ ХМАРИ

Призначення хмари визначається багатьма експертами, але визначення Національного інституту стандартів і технологій (NIST) є загальноприйнятим стандартом: «Хмарні обчислення - це модель, що дозволяє зручно відкрити мережевий доступ за запитом до загального пулу конфігурованих обчислювальних ресурсів (наприклад, мереж, серверів, сховищ, додатків і послуг), які можна швидко забезпечити і звільнити з мінімальними зусиллями з управління або взаємодією з постачальником послуг[4]. Простіше кажучи, хмара може вважатися набором апаратних засобів, програмного забезпечення та інших ресурсів, які можуть бути доступні через Інтернет, і використовуватися для збирання рішення за вимогою (тобто на момент запиту) для надання набору послуг назад запитувачу.

Багато практикуючих в комерційній та академічній сферах намагалися визначити, що таке «хмарні обчислення» і які унікальні характеристики він представляє. Buyya et al. [9] визначили його наступним чином: «Хмара - це паралельна і розподілена обчислювальна система, що складається з набору взаємопов'язаних і віртуалізованих комп'ютерів, які динамічно забезпечуються і представлені як один або більше уніфікованих обчислювальних ресурсів на основі угод про рівень обслуговування) встановлюється шляхом переговорів між постачальником послуг та споживачами. ”Vaquero et al. [10] заявили, що «хмари - це великий пул легко використовуваних і доступних віртуалізованих ресурсів (таких як апаратні засоби, платформи розробки та / або послуги). Ці ресурси можуть бути динамічно переконфігуровані, щоб пристосуватися до змінної навантаження (масштабу), що дозволяє також оптимально використовувати ресурси. Цей пул ресурсів, як правило, використовують

модель оплати за використання, в якій гарантії пропонуються постачальником інфраструктури за допомогою індивідуальних угод про рівень обслуговування. "

Хоча існує незліченна кількість інших визначень, видається, що існують спільні характеристики між найбільш помітними переліченими вище, які хмара повинна мати: (i) оплата за використання (без постійних зобов'язань, цін на комунальні послуги); (ii) еластичність і ілюзія нескінченних ресурсів; (iii) інтерфейс самообслуговування; та (iv) ресурси, які абстрагуються або віртуалізовані.

Окрім обчислень та зберігання, постачальники хмарних обчислень зазвичай пропонують широкий спектр програмних послуг. Вони також включають API та засоби розробки, які дозволяють розробникам створювати безліч масштабованих програм на своїх службах. Кінцева мета - дозволити клієнтам керувати своєю щоденною IT-інфраструктурою «в хмарі». Багато ажіотажу оточили область хмарних обчислень у зародковому стані, що часто вважається найважливішим перемикачем у світі IT після появи Інтернету [12].]. В середині такої реклами виникає велика плутанина, коли ви намагаєтеся визначити, що таке хмарні обчислення, і які обчислювальні інфраструктури можна назвати «хмарами». Справді, давня мрія про постачання комп'ютерів як утиліти була реалізована за допомогою поява хмарних обчислень [11].

Проте, протягом багатьох років, кілька технологій дозріли і значно сприяли життєздатності хмарних обчислень. У цьому напрямку це втілення відстежує коріння хмарних обчислень шляхом опитування основних технологічних досягнень, які значною мірою сприяли появі цієї нової галузі. Вона також пояснює концепції та розробки, класифікуючи та порівнюючи найбільш відповідні зусилля в галузі НДД у сфері хмарних обчислень, особливо громадські хмари, інструменти управління та рамки розробки. Перераховані найбільш значні практичні реалізації хмарних обчислень, з особливим акцентом на архітектурні аспекти та інноваційні технічні особливості.

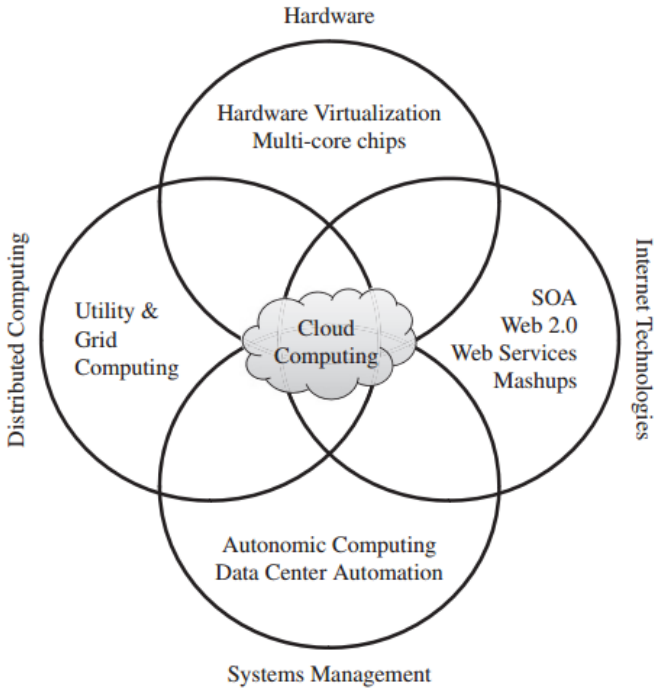


Рисунок 1.1 - Зближення різних досягнень, що призводять до появи хмарних обчислень

Ця модель приносить користь як споживачам, так і постачальникам послуг IT. Споживачі можуть досягти скорочення витрат, пов'язаних з інформаційними технологіями, шляхом вибору більш дешевих послуг від зовнішніх постачальників, а не значних інвестицій в IT-інфраструктуру та найм персоналу. Компонент «на вимогу» даної моделі дозволяє споживачам адаптувати своє використання IT до швидко зростаючих або непередбачуваних комп'ютерних потреб. Постачальники IT-послуг досягають кращих експлуатаційних витрат; апаратні та програмні інфраструктури побудовані для забезпечення декількох рішень і служать багатьом користувачам, таким чином підвищуючи ефективність і в кінцевому підсумку призводячи до більш швидкого повернення інвестицій (ROI), а також зниження загальної вартості володіння (TCO).

1.1 Цілі хмарних обчислень

Хмарні обчислення пропонують ціннісні пропозиції, які відрізняються від традиційних корпоративних IT-середовищ. Запропонуючи спосіб використання віртуалізації та сукупних обчислювальних ресурсів, хмарні обчислення можуть запропонувати економію масштабу, яка інакше була б недоступною. Він також може запропонувати можливості для негайного використання встановленого обладнання та програмного забезпечення, а не витрачати час і ресурси на розробку, розгортання і тестування нової реалізації.

Оскільки віртуальні екземпляри можуть бути забезпечені і припинені в будь-який час, а організація користувача сплачує тільки за використовувані обчислювальні ресурси, витрати можуть бути нижчими. Аналогічно, структури зборів повинні бути належним чином роз'яснені та зрозумілі для оцінки майбутніх витрат.

Переваги хмарних обчислень є переконливими:

– хмарні обчислення дозволяють витратам інфраструктури та її управління стати операційними витратами, а не капіталом;

– це може бути корисним для бізнесу як з податкової точки зору, так і тому, що дозволяє організації зберігати капітал для інших цілей[15];

– хмарні обчислення пропонують централізований, віддалений об'єкт для обчислень, що призводить до економії масштабу як у використанні апаратного та програмного забезпечення, так і до скорочення необхідних ресурсів для адміністративного управління;

– можливість негайного використання обчислювальних ресурсів, а не необхідність спочатку інвестувати час і кваліфіковані ресурси у розробку, впровадження та тестування інфраструктури (апаратне і проміжне програмне забезпечення). Це призводить до прискорення вартості, що може означати

збільшення доходу, більшу гнучкість бізнесу, більшу частку ринку або інші переваги;

– хмарні обчислення не існують у вакуумі. Більшість організацій матимуть широкий спектр програм, які вже працюють у своєму центрі обробки даних. Для більшості, хмарні обчислення розширять існуючу інфраструктуру. Вона може бути використана в основному для нових проектів. Або організація може використовувати її для переповнення, що гарантує певний рівень продуктивності для обчислень на підприємствах.

Рисунок 1.2 - Хмарні обчислення

1.2 Архітектура та підходи хмарних обчислень

Хмарна архітектура, системна архітектура програмних систем передбачає доставку хмарних обчислень, зазвичай включає в себе кілька компонентів

хмарного зв'язку, які спілкуються один з одним через вільний механізм зв'язку, наприклад, чергу обміну повідомленнями. Еластичне положення передбачає інтелект при використанні жорстких або вільних зв'язків, що застосовуються до таких механізмів, як ці та інші.

Головна архітектура хмарних обчислень:

1) основні характеристики хмарних обчислень:

– самообслуговування на вимогу;
– широкий доступ до мережі;
– об'єднання ресурсів;
– незалежність від розташування;
– здатність до масштабування;

2) моделі хмарніх служб:

– програмне забезпечення як послуга (SaaS);
– використовуйте програми постачальника через мережу;
– платформа як послуга (PaaS);
– розгортайте створені клієнтом програми в хмарі;
– інфраструктура як послуга (IaaS);
– оренда, зберігання, пропускна здатність мережі;

3) моделі розгортання хмар:

– громадсько-продаваної, мегамасштабна інфраструктура;
– приватне підприємство належить або орендується;
– гібридна композиція з двох або більше хмар;
– інфраструктура спільного використання.

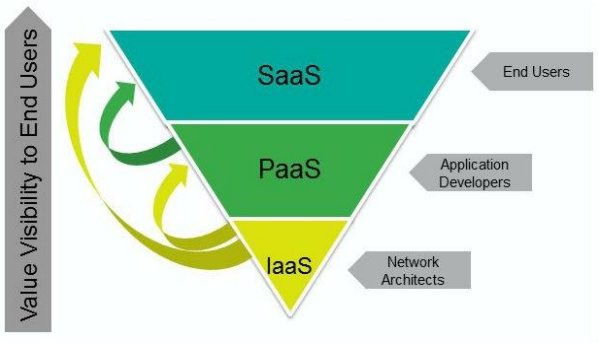


Рисунок 1.3 – Архітектура хмарних обчислень

Виділемо наступні характеристики хмарних обчислень:

– Самообслуговування на вимогу. Споживач може в односторонньому порядку надавати обчислювальні можливості, такі як час на сервері та мережеве сховище, у разі потреби, без необхідності взаємодії з кожним постачальником послуг;

– Широкий доступ до мережі. Можливості доступні через мережу і доступні через стандартні механізми, які сприяють використанню на різнорідних тонких або товстих клієнтських платформах (наприклад, мобільні телефони, планшети, ноутбуки та робочі станції);

– Об'єднання ресурсів. Обчислювальні ресурси постачальника об'єднуються для обслуговування декількох споживачів з використанням моделі з декількома орендарями, причому різні фізичні та віртуальні ресурси динамічно призначені та перепризначені відповідно до споживчого попиту. Існує відчуття незалежності розташування в тому, що клієнт взагалі не має контролю або знань щодо точного розташування наданих ресурсів, але може бути в змозі вказати місце розташування на більш високому рівні абстракції (наприклад, країна, стан або центр обробки даних). Приклади ресурсів включають зберігання, обробку, пам'ять і пропускну здатність мережі;

– Швидка еластичність. Можливості можуть бути еластично забезпечені і звільнені, в деяких випадках автоматично, для швидкого масштабування назовні

і всередину, співмірних попиту. Для споживача можливості, доступні для надання послуг, часто виявляються необмеженими і можуть бути використані в будь-якій кількості в будь-який час;

– Масштабуема послуга. Хмарні системи автоматично контролюють і оптимізують використання ресурсів, використовуючи можливість вимірювання на певному рівні абстракції, що відповідає типу послуги (наприклад, зберігання, обробка, пропускна здатність і активні облікові записи користувачів). Як правило, це робиться на основі оплати за використання або збору за використання. Використання ресурсів можна контролювати, контролювати і повідомляти, забезпечуючи прозорість як для постачальника, так і для споживача використовуваної послуги.

Існують такі моделі хмарних служб:

– Програмне забезпечення як послуга (SaaS). Можливості, що надаються споживачеві, - це використання додатків постачальника, що працюють на хмарній інфраструктурі. Програми доступні з різних клієнтських пристроїв через інтерфейс тонкого клієнта, наприклад веб-браузер (наприклад, веб-адресу електронної пошти) або інтерфейс програми. Споживач не керує та не контролює основну хмарна інфраструктура, включаючи мережу, сервери, операційні системи, сховище або навіть окремі можливості програми, за винятком обмежених для користувача налаштувань конфігурації програми;

– Platform as a Service (PaaS). Можливості, що надаються споживачеві, - це розгортання на хмарні інфраструктури створених або придбаних програм, створених з використанням мов програмування, бібліотек, служб і інструментів, що підтримуються постачальником. Споживач не управляє та не контролює базову хмарна інфраструктура, включаючи мережу, сервери, операційні системи або сховище, але має контроль над розгорнутими додатками та, можливо, конфігураційними параметрами для середовища хостингу додатків;

– Infrastructure as a Service (IaaS). Можливість, що надається споживачеві, полягає в забезпеченні обробки, зберігання, мереж та інших основних обчислювальних ресурсів, де споживач може розгортати і запускати довільне програмне забезпечення, яке може включати операційні системи і програми. Споживач не керує або керує базовою хмарою, але має контроль над операційними системами, сховищами та розгорнутими додатками; і, можливо, обмежений контроль вибраних компонентів мережі (наприклад, брандмауери хоста);

Моделі розгортання хмар:

– Приватне хмара. Хмарна інфраструктура передбачена для ексклюзивного використання однією організацією, що складається з кількох споживачів (наприклад, бізнес-одиниць). Воно може бути власною, керованою та керованою організацією, третьою стороною або деякою їх комбінацією, і воно може існувати на або поза приміщенням;

– Хмара спільноти. Хмарна інфраструктура передбачена для ексклюзивного використання певною спільнотою споживачів з організацій, які поділилися проблемами (наприклад, місія, вимоги безпеки, політика та вимоги до дотримання). Він може перебувати у власності, керуванні та керуванні однією або кількома організаціями спільноти, третьою стороною або деякою їх комбінацією, і він може існувати на або поза приміщенням;

– Публічне хмара. Хмарна інфраструктура забезпечується для відкритого використання широкою громадськістю. Воно може бути власною, керованою та керованою бізнесовою, академічною або державною організацією або деякою їх комбінацією. Вона існує в приміщенні постачальника послуг у хмарі;

– Гібридна хмара. Хмарна інфраструктура - це складова двох або більше чітких хмарних інфраструктур (приватних, громадських чи громадських), які залишаються унікальними об'єктами, але пов'язані між собою стандартизованою

або запатентованою технологією, що дозволяє переносити дані та додатки (наприклад, хмари для балансування навантаження між хмарами).

1.3 Проблеми та рішення

1.3.1 Хмарні обчислення безпеки

Основні посилання на керівництво безпекою та аналіз вищих загроз висвітлюють різні питання безпеки, пов'язані з хмарними обчисленнями, які потребують подальших досліджень для відповідного оброблення, а отже, для підвищення прийнятності та прийняття технологій. Особлива увага приділяється розмежуванню послуг у вигляді програмного забезпечення (SaaS), платформи (PaaS) та інфраструктури (IaaS), які зазвичай використовуються як фундаментальна основа для класифікації хмарних сервісів. Однак, жодні інші методи не стандартизовані або навіть застосовані для організації аспектів безпеки хмарних обчислень, крім моделей розгортання, типів послуг або традиційних моделей безпеки. З метою концентрації та організації інформації, пов'язаної з безпекою в хмарах, а також для полегшення майбутніх досліджень, у цьому розділі ми визначаємо основні проблеми в даній області та групуємо їх у модель, що складається з семи категорій, на основі згаданих вище посилань. Зокрема, категоріями є: мережева безпека, інтерфейси, безпека даних, віртуалізація, управління, відповідність і правові питання. Кожна категорія включає в себе декілька потенційних проблем безпеки, що призводить до класифікації підрозділів, що висвітлює основні проблеми, визначені в базових посиланнях.

1.3.2 Безпека мережі

Проблеми, пов'язані з мережевими комунікаціями та конфігураціями щодо інфраструктур хмарних обчислень. Ідеальним рішенням для забезпечення безпеки мережі є наявність хмарних сервісів як розширення існуючих внутрішніх мереж клієнтів, прийняття тих самих заходів захисту та заходів безпеки, які реалізовані на місцевому рівні та дозволяють їм розширювати локальні стратегії на будь-який віддалений ресурс або процес:

– Забезпечення передачі: Синхронізація розподілених архітектур, масового обміну ресурсами та синхронізації екземплярів віртуальних машин (VM) передбачає більшу кількість транзитних даних у хмарі, що вимагає механізмів VPN для захисту системи від перехоплення, спуфінга, атак в середині та з боку каналу;

– Firewalling: Брандмауери захищають внутрішню хмарну інфраструктуру провайдера від інсайдерів та аутсайдерів. Вони також дозволяють ізоляцію віртуальної машини, тонкозернисту фільтрацію для адрес і портів, запобігання DoS і виявлення зовнішніх процедур оцінки безпеки. Зусилля з розробки послідовного брандмауера та подібних заходів безпеки, характерних для хмарних середовищ, виявляють бажання адаптувати існуючі рішення для цієї нової комп'ютерної парадигми;

– Конфігурація безпеки: Конфігурація протоколів, систем і технологій для забезпечення необхідних рівнів безпеки та конфіденційності без погіршення продуктивності або ефективності;

1.3.3 Інтерфейси

Концентруе всі питання, пов’язані з користувальницькими, адміністративними та програмувальними інтерфейсами для використання та управління хмарою:

– API: інтерфейси програмування (необхідні для IaaS і PaaS) для доступу до віртуалізованих ресурсів і систем повинні бути захищені, щоб запобігти зловмисному використанню;

– Інтерфейс адміністрування: дає можливість дистанційного керування ресурсами в IaaS (управління VM), розробки для PaaS (кодування, розгортання, тестування) і прикладних засобів для SaaS (управління доступом користувача, конфігурації);

– Інтерфейс користувача: Інтерфейс кінцевого користувача для вивчення наданих ресурсів і інструментів (сама послуга), що передбачає необхідність прийняття заходів для захисту навколишнього середовища.

– Аутентифікація: Необхідні механізми для доступу до хмари. Більшість послуг покладаються на регулярні рахунки, тому вони сприйнятливі до безлічі атак, наслідки яких підсилюються багаторазовим орендою та розподілом ресурсів;

1.3.4 Безпека данних

Захист данних з точки зору конфіденційності, доступності та цілістності(що може бути застосовано не тільки до хмарних середовищ, але і до будь-якого рішення, що вимагає базових рівнів безпеки)

– Криптографія: Найбільш поширена практика для забезпечення конфіденційних даних, ретельно необхідних галузевими, державними і федеральними правилами.

– Надмірність: необхідна для уникнення втрати даних. Більшість бізнес-моделей спираються на інформаційні технології для своїх основних функціональних можливостей і процесів, а отже, необхідно забезпечити цілісність і доступність критично важливих даних.

– Утилізація: Елементарні способи видалення даних є недостатніми і зазвичай називаються видаленням. У хмарі повне знищення даних, включаючи посилання на журнали та приховані резервні реєстри, є важливою вимогою.

1.3.5 Віртуалізація

Ізоляція між ВМ, уразливостями гіпервізора та іншими проблемами, пов’язаними з використанням технологій віртуалізації:

– Ізоляція: Хоча логічно ізольовані, всі віртуальні машини мають однакове обладнання і, отже, однакові ресурси, що дозволяє зловмисним об'єктам використовувати витоки даних і атаки між віртуальною машиною. Концепція ізоляції також може бути застосована до більш дрібнозернистих активів, таких як обчислювальні ресурси, зберігання та пам'ять.

– Уразливості гіпервізора: Гіпервізор є основним програмним компонентом віртуалізації. Незважаючи на наявність відомих уразливостей безпеки для гіпервізорів, рішення все ще залишаються дефіцитними і часто є власністю, що вимагає подальших досліджень для посилення цих аспектів безпеки.

– Витік даних: Використовуйте уразливості гіпервізорів та відсутність контролю ізоляції, щоб пропускати дані з віртуалізованих інфраструктур, отримувати конфіденційні дані клієнтів і впливати на конфіденційність та цілісність.

– Ідентифікація віртуальної машини: відсутність елементів керування для ідентифікації віртуальних машин, які використовуються для виконання певного процесу або для зберігання файлів.

– Атаки крос-віртуальних машин: включає спроби оцінити швидкість трафіку постачальника, щоб викрасти криптографічні ключі та збільшити шанси на атаки розміщення VM. Одним з прикладів є перекриття областей пам'яті та зберігання, спочатку призначених для однієї віртуальної машини, що також дає можливість іншим атакам, пов'язаним з ізоляцією.

1.5.6 Управління

Питання, пов’язані з (втратою) адміністративним контролем та контролем безпеки в рішеннях хмарних обчислень:

– Керування даними: Переміщення даних у хмару означає втрату контролю над надмірностями, розташуванням, файловими системами та іншими відповідними конфігураціями.

– Контроль безпеки: втрата управління механізмами та політикою безпеки, оскільки умови використання забороняють оцінку вразливості на стороні клієнта та тести на проникнення, а недостатні угоди про рівень обслуговування (SLA) призводять до недоліків безпеки.

– Блокування: потенційна залежність користувача від конкретного постачальника послуг через відсутність усталених стандартів (протоколів і форматів даних), що стає особливо вразливим для міграції та припинення служби.

1.3.7 Відповідність

Включає вимоги, пов’язані з доступністю послуг та можливостями аудиту.

– Угоди про рівень обслуговування (SLA): механізми, що забезпечують необхідну доступність послуг та основні процедури безпеки, які необхідно прийняти.

– Втрата сервісу: перебої в обслуговуванні не є виключними для хмарних середовищ, але є більш серйозними в цьому контексті через взаємозв'язок між службами (наприклад, SaaS з використанням віртуальних інфраструктур, наданих IaaS), як показано в багатьох прикладах. Це призводить до необхідності сильної політики відновлення після аварії та рекомендацій постачальників для реалізації надмірності на стороні клієнта, якщо це можливо.

– Аудит: Дозволяє проводити оцінку безпеки та доступності клієнтами, постачальниками та третіми сторонами. Прозорі та ефективні методології необхідні для постійного аналізу умов обслуговування та, як правило, вимагаються контрактами або правовими нормами. Існують рішення, розроблені для вирішення цієї проблеми, пропонуючи прозорий API для автоматизованого аудиту та інші корисні функціональні можливості.

– (d) Відповідність сервісу: Що стосується того, як договірні зобов'язання та загальні вимоги до послуг поважаються і пропонуються на основі визначених та базових послуг та потреб клієнтів.

1.3.8 Складність

До цього часу були запропоновані численні системи керування ідентифікацією хмар (IDMS); однак, більшість цих систем не є ні широко прийнятими, ні вважаються високонадійними через їх обмеження з точки зору обсягу, застосовності та безпеки. Для досягнення надійності та ефективності в IDMs для Cloud, необхідно проводити подальші великі дослідження для критичного вивчення IDMS на основі хмари та їх рівня безпеки.

Іншим аспектом систем Cloud є складність. Проблема розуміння хмарних систем випливає з того, що їх просто моделювати досить складно. Cloud є дуже динамічною системою з численними користувачами, пристроями та мережами, що з'єднують і відключають одночасно з хмарою. Ця складність до такої міри, що її можна порівняти зі складністю людського мозку, де нейрони безперервно з'єднуються і змінюють свою синаптичну структуру для зберігання інформації.

Проте, проблема тут полягає в тому, що на відміну від мозку, де сполучні нейрони вже пройшли аутентифікацію, хмарні системи вимагають великої аутентифікації, а також систем управління ідентифікацією. Тим не менш, цього просто не достатньо для задоволення постійно зростаючих вимог нових парадигм, таких як Інтернет речей (IoT) у зв'язку з його зв'язком з хмарою.

1.3.9 Стандартизація хмарних обчислень

Відсутність стандартів може зробити обчислювальну техніку більш складною для використання. Вона також може обмежити впровадження, обмеживши взаємодію між хмарними платформами і викликаючи непослідовність у таких сферах, як безпека та сумісність. Наприклад, відсутність стандартизації може призвести до того, що клієнт намагатиметься перейти від привілейованого до загальнодоступного хмари від того, щоб зробити це так само легко, як перемикання браузерів або систем електронної пошти. Крім того, це дозволить користувачам не знати про основні можливості, які вони можуть очікувати від будь-яких хмарних сервісів.

Сумісність між пропозиціями та портативністю послуг від одного постачальника до іншого дуже важлива для клієнта, щоб максимізувати очікувану прибутковість від хмарних обчислень. Відсутність стандартів безпеки - вирішення таких питань, як конфіденційність даних і шифрування - також завдає шкоди широкому прийняттю обчислювальної техніки.

1.3.10 Стандартизація хмари.

Найосновніше, хмара обчислень просто доставка програм; охоронні та інші послуги; складські та інші інфраструктури; і плати, такі як розробки програмного забезпечення для користувачів через Інтернет або приватне хмара.

Хмарні обчислення залучені до багатьох організацій, оскільки це мінімізує кількість апаратних засобів та програмного забезпечення, які користувачі повинні володіти, підтримувати та оновлювати. По суті,

користувачі платять тільки за необхідні обчислювальні можливості. Істинна сумісність вимагає перекладу конкретної функціональності програми та сервісу з однієї хмари на іншу, і це не відбудеться без стандартизації.

Ключовим питанням стандартизації є віртуалізація, яка відіграє важливу роль у більшості підходів до обчислення хмар. Гнучкість віртуалізації дозволяє постачальникам послуг хмари оптимізувати робочі навантаження серед своїх апаратних ресурсів. Це також дає можливість користувачам, наприклад, користуватися ними; підключитися до сховища без необхідності знати про імена серверів і адреси, що було б у традиційній мережі.

У віртуалізації гіпервізори керують обробкою хост-сервера та іншими ресурсами, так що він може запускати кілька віртуальних машин (ВМ), використовуючи різні операційні системи та інші платформи. Кожна хмарна платформа має свій тип гіпервізора. Хмарні системи, що використовують різні гіпервізори, не взаємодіють між собою, частково через те, що вони не використовують однакові формати даних.

Хмарні платформи також не взаємодіють, оскільки їхні віртуальні машини не взаємодіють стандартним чином з різними архітектурами мережі, архівами, API, мережевими підключеннями, базами даних та іншими елементами. Переклад VM є важливим питанням для забезпечення збереження політики безпеки, політики мережі та ідентичності в хмарах. Без стандартизації, перенесення робочого навантаження з однієї платформи хмари на іншу потребує створення нової віртуальної машини на другій платформі, а потім перевстановлення програми, що може зайняти значний час і зусилля.

2 ТЕОРЕТИЧНІ ДОСЛІДЖЕННЯ

Винайдення Інтернету змінює спосіб використання комп'ютера. Від пошти до магазину ми всі залежать від цієї величезної групи мережевого комп'ютера. Хмарні обчислення повністю змінює те, що означає Інтернет. Погана програма для настільних комп'ютерів доступна в мережі, а пам’ять доступна в Інтернеті в будь-якому місці з будь-якого пристрою. Навчання та веб 2.0 навчання повністю змінює систему освіти. Вчитель і студент працюють разом в онлайн-проекті не в школі або в коледжах, а з дому також. Викладання ніколи не було легким без хмарних обчислень [10].

Відкритий університет поступово розвивається в електронний університет вже більше десяти років, впроваджуючи нові курси, які вимагають доступу до ПК та Інтернету, пропонуючи більше можливостей ІКТ в інших курсах. Поєднання курсів та засобів масової інформації стає все більш різноманітним. Те, що характеризує підтримувану модель відкритого навчання, зараз зосереджується на відповідних засобах масової інформації, залежно від цілей, характеру матеріалу та цільової студентської популяції. Вивчення того, що вважається доречним, є безперервним процесом, який буде актуальним для всіх інших університетів, які бажають розвивати електронне навчання. Це важке завдання охопити все, що ми дізналися про електронний університет, в просторі однієї статті. Далі йде вибіркове пояснення, яке зосереджується на деяких найважливіших елементах нашого виживання в е-світі.

Становлення електронного університету означає збільшення складності навчання та викладання. Це означає розширення можливостей існуючих систем і персоналу. Це також має означати підвищення ступеня задоволення потреб студентів, як академічних, так і логістичних - інакше чому ми це робимо? Підсумовуючи деякі з найбільш важливих уроків, отриманих за останні кілька

років інновацій: студенти цінують активне середовище навчання та підтримки, яке пропонує ІКТ:

– ми повинні зосередитися на досягненні правильного балансу між ІКТ та не-ІКТ, між інтерактивними вправами та комунікативною, спільною роботою в Інтернеті;

– ми повинні керувати очікуваннями попиту на більш інноваційні та більш досконалі матеріали, а також забезпечувати надійне середовище для обслуговування та доставки для них;

– планування робочого навантаження для студентів має важливе значення для уникнення відмови від навчання; планування робочого навантаження для персоналу має важливе значення для забезпечення сталого розвитку, використовуючи такі технології, як перепрофілювання та налаштування; Викладацький персонал потребує більше допомоги та підтримки від фахівців;

– академічні та допоміжні працівники повинні робити більше науково-дослідних робіт та інновацій у навчанні - і це має бути визнане та винагороджене;

– забезпечення якості, що забезпечує зворотній зв'язок з усією діяльністю, пов'язаною з ІКТ, забезпечить необхідність постійного вдосконалення процесу.

Будь-який університет, який розглядає можливість переходу на електронне навчання, повинен вирішувати всі ці питання і відкривати культуру інновацій та досліджень у процесі навчання та викладання. Спільнота Відкритого Університету має високу чутливість до електронних послуг, і це буде поширюватися на інші ВНЗ, які бажають перейти на електронне навчання для неповного, дорослого, безперервного навчання. Що б ми не пропонували, існує величезне поглинання і попит на більше. Однак ІКТ є дуже трудомістким. У короткостроковій перспективі, принаймні, зростають витрати. Ми повинні контролювати витрати, якщо новий бізнес має бути сталим.

Тому нам потрібно постійне вдосконалення процесу, для онлайн-послуг і для виробництва матеріалів. Важливо зберегти баланс між ІКТ та не-ІКТ. Ми повинні чітко розуміти поняття «електронного університету» та «електронного навчання». У Відкритому Університеті, ми зрозуміли, що ми не визначені з точки зору технології, яку ми використовуємо. У 1960-х роках наші засновники відмовилися бачити нас як «Університет Повітря». Ми не збираємося стати «Університетом Мережі». Для університетів важливо визначити їхні основні цінності. Незважаючи на те, що ми можемо працювати з концепцією електронного університету, ми повинні залишатися, в принципі, університетом, відповідальним за дослідження, науку і навчання. Засоби, за допомогою яких ми виконуємо ці основні заходи, залишаються несподіваними для них.

2.1 Види хмарних обчислень у університетах

Сервіс обчислень у хмарі, який дозволить університетам і коледжам створювати власні приватні хмари, які можуть бути інтегровані в громадські хмарні сервіси [10]. Три основні фактори інтересів Cloud Computing: 1) швидке зниження вартості апаратних засобів і збільшення обчислювальної бідності та можливостей зберігання, а також поява багатоядерної архітектури і сучасних суперкомп'ютерів, що складаються з сотень тисяч ядер; 2) експоненціально зростаючий обсяг даних у наукових інструментах / моделюванні та Інтернет-публікації та архівації; 3) широке впровадження програм Computing і Web 2.0. Наприклад, студент університету, що навчається в коледжі, може отримати доступ до хмари зі своєї двері, щоб отримати фізичний або віртуальний сервер (з необхідною пам'яттю), а також скопіювати програмне забезпечення Maple або MATLAB, яке використовується для виконання домашньої роботи або проект

класу. Крім того, вчитель початкової школи може отримати доступ до однієї хмари, щоб запросити одну віртуальну машину для кожного з своїх учнів, які працюють з програмним забезпеченням з математики, як частину навчальної діяльності в класі [12].

Нещодавнє дослідження, проведене компанією KPMG, виявило, що 81% підприємств, які оцінюють хмарні послуги, запланували впровадження хмари або вже реалізували стратегію хмари. Чотири з десяти сказали, що вони не мали негайних планів розпочати використання хмари. Незалежно від того, як бізнес вирішить перейти до хмари, ясно одне: вони переходять до хмари.

Завдяки технології хмарних обчислень великі резерви ресурсів можуть бути підключені через приватні або громадські мережі. Ця технологія спрощує планування інфраструктури і забезпечує динамічно масштабовану інфраструктуру для хмарних додатків, даних і зберігання файлів. Підприємства можуть вибрати розгортання додатків на публічних, приватних, гібридних хмарах або хмарах спільноти.

Які відмінності між цими типами хмарних обчислень і як ми можемо визначити правильний хмарний шлях для нашої організації? Ось деякі основні елементи кожного з них, щоб допомогти у процесі прийняття рішень.

2.1.1 Публічна хмара

Публічні хмари стають доступними для широкої громадськості постачальником послуг, який розміщує хмарну інфраструктуру. Як правило, публічні постачальники хмари, такі як Amazon AWS, Microsoft і Google, володіють та управляють інфраструктурою та пропонують доступ через Інтернет. З цією моделлю, клієнти не мають видимості або контролю над тим,

де знаходиться інфраструктура. Важливо відзначити, що всі клієнти на громадських хмарах мають спільний пул інфраструктури з обмеженою конфігурацією, захистом безпеки та відхиленнями в доступності.

Громадські клієнти в хмарі отримують вигоду від економії на масштабі, оскільки витрати на інфраструктуру розподілені між усіма користувачами, що дозволяє кожному окремому клієнту працювати на дешевій моделі «pay-as-we-go». Ще одна перевага інфраструктур публічної хмари полягає в тому, що вони зазвичай більші за масштаби, ніж власне корпоративне хмара, яка надає клієнтам плавну масштабованість на вимогу. Ці хмари забезпечують найбільший рівень ефективності спільних ресурсів; однак вони також є вразливішими, ніж приватні хмари.

Публічне хмара - це очевидний вибір, коли:

– ми стандартизовані навантаження для додатків використовується багатьма людьми, такими як електронна пошта;

– нам необхідно перевірити і розробити код програми;

– нам потрібні додаткові можливості (можливість додавання обчислювальних ресурсів у часи пік).

2.1.2 Приватна хмара для університетів

Приватна хмара - це хмарна інфраструктура, присвячена певній організації. Приватні хмари дозволяють підприємствам розміщувати програми в хмарі, одночасно вирішуючи питання щодо безпеки та контролю даних, яких часто не вистачає в публічному хмарі. Вона не ділиться з іншими організаціями, незалежно від того, керується вона внутрішньо або третьою стороною, і може бути розміщена на внутрішньому або зовнішньому каналі:

– Приміщення Приватне Хмара: Цей тип хмари розміщується в межах власних організацій. IT-відділ підприємств зазнає капітальних і експлуатаційних витрат на фізичні ресурси з цією моделлю. Приміщені приватні хмари найкраще використовуються для додатків, які вимагають повного контролю та налаштування інфраструктури та безпеки.

– Зовнішнє розміщення приватного хмари: приватні хмари, що розміщуються зовні, також використовуються тільки однією організацією, але розміщуються третьою стороною, що спеціалізується на інфраструктурі хмари. Постачальник послуг сприяє ексклюзивному хмарному середовищу з повною гарантією конфіденційності. Цей формат рекомендується для організацій, які вважають за краще не використовувати інфраструктуру публічної хмари через ризики, пов'язані з розподілом фізичних ресурсів.

Приватна хмара (яка також називається внутрішньою хмарою або корпоративною хмарою) є маркетинговим терміном для власної архітектури обчислень, яка надає хостинг для обмеженого числа людей за брандмауером. Досягнення у сфері віртуалізації та розподілених обчислень дозволили адміністраторам корпоративних мереж та центрів обробки даних ефективно стати постачальниками послуг, які задовольняють потреби своїх клієнтів у корпорації. Маркетингові засоби масової інформації, які використовують слова "приватне хмара", розраховані на те, щоб звернутися до організації, яка потребує або хоче отримати більший контроль над їхніми даними, ніж вони можуть отримати за допомогою сторонніх послуг, таких як Elastic Compute Cloud (EC2) або просте сховище Amazon Служба (S3) [6]. Рис. 2.1.2. Представляють приватну хмару організації.

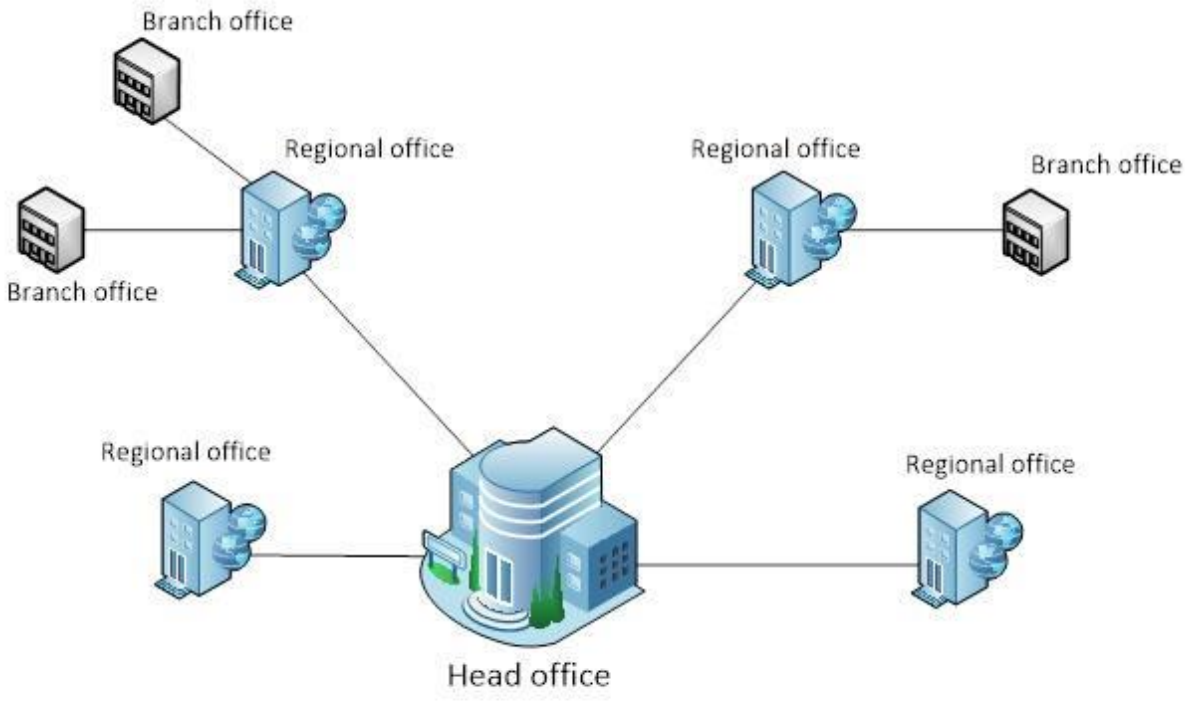


Рисунок 2.1 - Приклад приватної хмари в організаціях

При аналізі визначень існує консенсус щодо кількох ключових моментів; (1) Хмарні обчислення забезпечують доступ до пулу обчислювальних ресурсів на вимогу, (2) динамічно масштабовані сервіси, (3) незалежність пристроїв і засобів масової інформації, і (4) легше обслуговування програм, які не потрібно встановлювати на користувачів 'комп'ютери. Хмарні обчислення повинні бути еластичністю і масштабованістю.

2.1.3 Гібрид

Гібридні хмари є складом двох або більше хмар (приватних, спільноти або громадськості), які залишаються унікальними об'єктами, але об'єднуються

разом, пропонуючи переваги декількох моделей розгортання. У гібридному хмарі ми можемо використовувати повні або часткові способи використання сторонніх постачальників хмари; підвищення гнучкості обчислень.

Збільшення традиційної приватної хмари за допомогою ресурсів публічної хмари може бути використано для управління будь-якими несподіваними сплесками навантаження.

2.1.4 Спільнота

Хмара спільноти - це модель мульти-орендарів, яка поділяється між кількома або організаціями і керується, керується та закріплюється зазвичай усіма учасниками організації або третім учасником, що управляє послугами.

Хмари спільноти - це гібридна форма приватних хмар, побудованих і експлуатованих спеціально для цільової групи. Ці спільноти мають схожі хмарні вимоги, і їхня кінцева мета - спільна робота для досягнення своїх бізнес-цілей.

Нижче наведено кілька ситуацій, в яких найкращим є середовище для спільноти:

– урядові організації в державі, які повинні розділити ресурси

– приватна ХІПА-сумісна хмара для групи лікарень або клінік

– хмара Telco спільноти для телекомунікаційної компанії DR для задоволення конкретних правил FCC

2.2 Використання хмарної платформи Amazon Web Services

AWS складається з багатьох хмарних сервісів, які ми можемо використовувати в комбінаціях, пристосованих до наших бізнес-або організаційних потреб. У цьому розділі представлені послуги AWS у таких категоріях: обчислювальні, мережеві, зберігання та доставка контенту, бази даних, аналітика, прикладні послуги, розгортання та управління, мобільні пристрої та програми.

2.2.1 Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) - це веб-сервіс, що забезпечує зміну розміру обчислювальної потужності в хмарі. Він розроблений для полегшення обчислень веб-масштабу для розробників і системних адміністраторів. Простий веб-інтерфейс Amazon EC2 дозволяє отримувати та налаштовувати ємність з мінімальним тертям. Вона забезпечує повний контроль над обчислювальними ресурсами і дозволяє нам працювати на перевіреному обчислювальному середовищі Amazon. Amazon EC2 скорочує час, необхідний для отримання та завантаження нових екземплярів сервера (так званих екземплярів Amazon EC2) до хвилин, що дозволяє нам швидко масштабувати потужність, як вгору, так і вниз, оскільки наші вимоги до обчислень змінюються. Amazon EC2 змінює економіку обчислювальної техніки, дозволяючи користувачеві платити тільки за фактично використану потужність. Amazon EC2 надає розробникам і системним адміністраторам інструменти для

побудови стійких до відмов прикладних програм і виділення від звичайних сценаріїв помилки.

Переваги Elastic Web-Scale Computing

Amazon EC2 дозволяє збільшувати або зменшувати потужність протягом декількох хвилин, а не годин або днів. Ми можемо одночасно вводити один, сотні або навіть тисячі серверних екземплярів. Звичайно, оскільки все це контролюється за допомогою API веб-служб, наша програма може автоматично масштабувати себе вгору і вниз залежно від його потреб.

Повністю керований

Ми можемо мати повний контроль над нашими екземплярами Amazon EC2. Вони мають корінний доступ до кожного з них, і ми можемо взаємодіяти з ними, як і будь-яка машина. Ми можемо зупинити наш примірник Amazon EC2, зберігаючи дані на нашому завантажувальному розділі, а потім перезапустити той самий екземпляр, використовуючи API веб-служби, повністю керований. Екземпляри можуть бути перезавантажені віддалено за допомогою API веб-служб. Крім того, ми можемо використовувати консоль керування AWS, простий, веб-інтерфейс користувача, для доступу та керування нашими екземплярами Amazon EC2.

Гнучкі хостингові послуги

Ми можемо вибрати один з декількох типів екземплярів Amazon EC2, операційних систем і програмних пакетів. Amazon EC2 дозволяє вибрати конфігурацію пам'яті, процесора, сховища екземплярів і розміру завантажувального розділу, який є оптимальним для нашого вибору операційної системи і програми. Наприклад, наш вибір операційних систем включає численні дистрибутиви Linux і Microsoft Windows Server.

Призначений для використання з іншими веб-службами Amazon

Amazon EC2 працює спільно з Amazon Simple Storage Service (Amazon S3), службою Amazon Relational Database (Amazon RDS), Amazon DynamoDB і

Amazon Simple Queue Service (Amazon SQS) для забезпечення комплексного рішення для обчислень, обробки запитів і зберігання широкий спектр застосування.

Надійний

Amazon EC2 пропонує високонадійне середовище, в якому можна швидко і передбачувано запровадити заміну екземплярів. Служба працює в перевіреній мережевій інфраструктурі Amazon і центрах обробки даних. Зобов'язання Amazon EC2 Service Level Agreement становить доступність 99,95% для кожної області Amazon EC2.

2.2.2 Amazon VPC

Віртуальна приватна хмара Amazon (Amazon VPC) дозволяє забезпечити логічно ізольований розділ хмари AWS, де ми можемо запускати ресурси AWS у віртуальній мережі, яку ми визначаємо. Ми маємо повний контроль над нашим віртуальним мережевим середовищем, включаючи вибір власного діапазону IP-адрес, створення підмереж і конфігурацію таблиць маршрутів і мережевих шлюзів. Ми можемо легко налаштувати конфігурацію мережі для нашої Amazon VPC. Наприклад, ми можемо створити громадську підмережу для наших веб-серверів, які мають доступ до Інтернету, і розміщувати наші системи, такі як бази даних або сервери додатків, в підмережі, що не мають доступу до Інтернету. Ми можемо використовувати декілька шарів безпеки (включаючи групи безпеки та списки контролю доступу до мережі), щоб допомогти контролювати доступ до екземплярів Amazon EC2 у кожній підмережі.

3 ПРОЕКТУВАННЯ ПРОГРАМНОЇ СИСТЕМИ

У цьому розділі описуються найкращі практики постачальників веб-додатків, що використовують хмару обчислень. Архітектурні елементи, описані в документі, необхідні для створення середовища хостингу веб-додатків, що використовує приватні, загальнодоступні або гібридні моделі розгортання хмари. На високому рівні, хостинг веб-додатків підтримує серверні програми, які доставляють веб-сторінки, що містять статичний і динамічний контент, через HTTP або HTTPS. Статичний вміст зазвичай представлений "шаблоном тексту" веб-сторінки і більш спеціалізованим контентом, що зберігається у файлах, таких як зображення, відео, звукові кліпи та документи PDF. Динамічний контент зазвичай будується у відповідь на конкретний запит від клієнта, заснований на контенті в запиті і змісті, отриманому з бази даних, підключеної до веб-додатку. Основним компонентом для розміщення веб-додатків є сервер веб-додатків, але для створення безпечної, надійної та високопродуктивної архітектури необхідний ряд інших компонентів, таких як брандмауери, балансування навантаження, бази даних, сховища файлів і мережі доставки контенту.

Крім того, для цих компонентів необхідно розглянути управління життєвим циклом, управління операціями та управління. Спосіб виконання цих функцій буде відрізнятися залежно від того, де розгортаються компоненти та як підтримується інтеграція в системи управління. Коли хмарний сервіс є пропозицією інфраструктури як послуги (IaaS), всі елементи архітектури повинні бути індивідуально придбані або інстанційно створені. У деяких випадках постачальник хмарних послуг IaaS може запропонувати деякі елементи в готовій формі. У випадку, коли хмарний сервіс є пропозицією

платформи як послуги (PaaS), часто буває, що багато елементів архітектури доступні як частина пропозиції та потрібна лише конфігурація та розгортання.

Модель розгортання хмари впливає на розташування багатьох компонентів. Для розгортання публічної хмари елементи створюються у публічному хмарі. Для розгортання приватної хмари компоненти створюються в приватній хмарі, або в локальній мережі, або в оточенні приватного керування, яке надає постачальник хмарних послуг. Для розгортання гібридної хмари існує елемент вибору місця розташування кожного компонента, або в загальнодоступному середовищі, або в приміщеннях, причому вибір, зазвичай, регулюється міркуваннями безпеки.

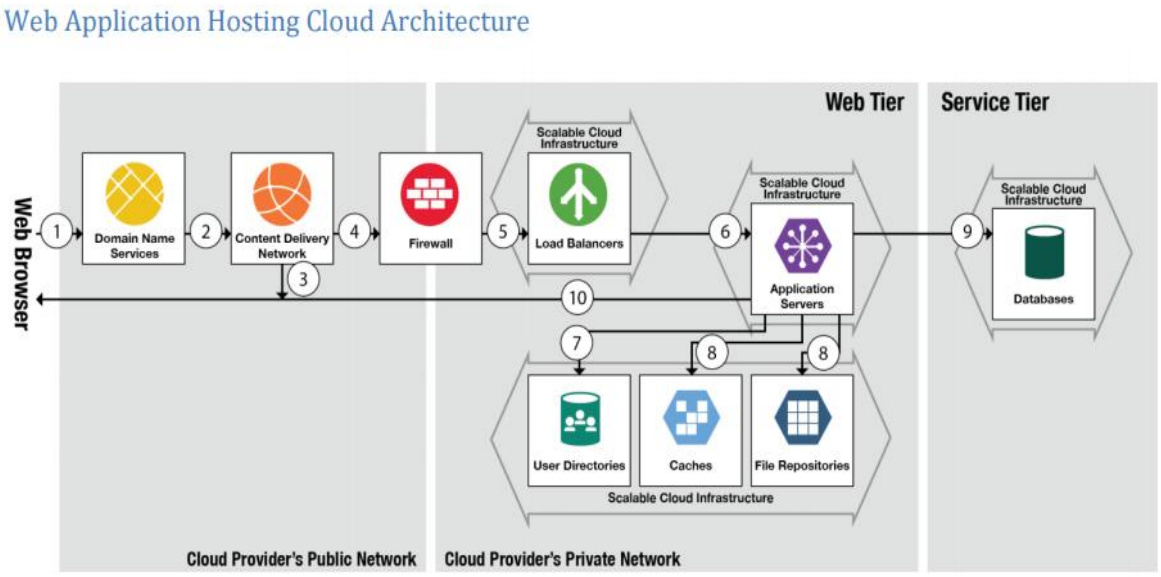


Рисунок 3.1- Хостинг веб-додатків Хмарної архітектури

Поля на рисунку 3.1 визначені в наступному розділі компонентів, а числа вказують порядок потоку.

Компоненти

Сервер DNS - Сервер доменних імен (DNS) вирішує текстову URL-адресу для певного веб-ресурсу на адресу TCP-IP системи або служби, яка може доставити цей ресурс клієнту.

Firewall - Firewall (Брандмауер) - це система, призначена для управління доступом до системи або з неї. Брандмауери можуть бути реалізовані як окреме виділене обладнання, або як компонент в інших мережевих пристроях, таких як балансування навантаження або маршрутизатор, або як інтегральне програмне забезпечення для операційної системи.

Balancer Load - балансування навантаження розподіляє трафік мережі або додатків через багато ресурсів (наприклад, комп'ютери, процесори, сховища або мережні посилання), щоб максимально збільшити пропускну здатність, мінімізувати час відгуку, збільшити потужність і підвищити надійність програм. Балансувачі навантаження можуть балансувати навантаження локально і глобально. Слід взяти до уваги, що цей компонент є високодоступним і не є єдиною точкою відмови.

Мережа доставки контенту (CDN) - Мережі доставки контенту - це географічно розподілені системи серверів, розгорнуті для мінімізації часу відгуку для обслуговування ресурсів географічно розподілених користувачів, забезпечуючи високий рівень доступності та доступності для користувачів з мінімальною затримкою. Які сервери задіяні будуть залежати від близькості сервера до користувача і місця, де вміст зберігається або кешується.

Кеш - кеші зберігають інформацію, тимчасово необхідну для виконання запиту сервером веб-додатків, включаючи дані сеансу та інший вміст. Метою кеш-пам'яті є зменшення затримки у відповідь на запит від клієнта.

File Repository - сховища файлів - це пристрої або програми, які зберігають інформацію, дані тощо у вигляді файлів. Доступ до сховища файлів зазвичай включає в себе можливість зберігати, отримувати, видаляти і шукати

сховище для конкретного файлу. Репозитарії файлів можуть використовувати мережеве сховище для забезпечення доступу до спільних файлів.

Сервери веб-додатків - сервери веб-додатків пропонують функціональність веб-сервера та інтегровану функціональність сервера додатків, якщо це необхідно. Веб-сервери - це системи, які повертають ресурси (наприклад, веб-вміст і зображення) у відповідь на запит HTTP і можуть бути налаштовані для обробки запитів для декількох IP-адрес і / або доменів. Інтегрований сервер додатків містить логіку програми, яка використовується для створення динамічного веб-вмісту. Це може включати отримання даних з файлів, баз даних, http-служб, датчиків та інших джерел даних, а також програмного генерування нових даних або інформації.

Сервери веб-додатків можуть підтримувати кластеризацію, об'єднання пулів та інші конфігурації високої доступності та масштабування, включаючи автоматичне масштабування - створення і видалення екземплярів сервера додатків, які вимагають потреби. Веб-сервери та сервери додатків також можуть бути створені в 3-шаровій установці з розділеними, а не інтегрованими веб-серверами та серверами додатків. У такому випадку були б окремі пули веб-серверів і серверів додатків, підключених через балансування навантаження. Сервер додатків відповідає за доступ до баз даних або інших систем.

Каталог користувачів - Каталог користувачів містить ідентифікатори користувача та облікові дані, необхідні для перевірки того, чи користувач має право на доступ до інформації або додатків, які запитуються на веб-серверах і серверах додатків. Доступ до каталогу може здійснюватися веб-серверами, серверами додатків, базами даних або будь-якими іншими елементами, що використовуються у веб-додатку.

База даних - бази даних - це структуровані набори даних. Зазвичай бази даних зберігаються на пристроях зберігання даних, підключених до комп'ютерів та / або мереж. Репліковані бази даних є стратегією для високодоступних і

надійних систем, в яких дані часто копіюються між 2 або більше базами даних, усуваючи вузькі місця і окремі точки відмови.

3.1 Архітектура системи

Архітектура архітектури хостингу веб-додатків відповідно до потоку чисел, вказаних відповідно на рис. 3.1.

1. Сервер доменних імен (DNS) - агент користувача (або користувач) надсилає запит на вказаний URL. Частина домену URL-адреси вирішується в IP-адресу за допомогою служби доменних імен (DNS). Ця IP-адреса може фактично являти собою IP-адресу сервера CDN, балансування навантаження, брандмауера або проксі-сервера перед фактичним сервером веб-додатків, який задовольнить запит.

2. Сервер CDN визначає, чи є який-небудь із запитуваного контенту в мережі зберігання CDN. Якщо сервер CDN не може задовольнити запит, запит надсилається до брандмауера.

3. Якщо сервер CDN здатний задовольнити запит, що використовує вміст в найближчій близькості до користувача, то CDN відповідає на запит, повертаючи цей вміст. Браузер користувача отримує та відображає повернений вміст.

4. Брандмауер - брандмауер оцінює пакети, які формують запит, і дозволяє цим пакетам продовжувати вперед до балансування навантаження, якщо вони відповідають правилам брандмауера. Типові правила можуть передавати тільки вхідні HTTP і HTTPS пакети, призначені для портів 80 і 443. Брандмауери часто мають два набори правил, один для трафіку за межами брандмауера і один для трафіку в брандмауері. Як правило, дозвіл DNS для

внутрішніх запитів зазвичай виконується за допомогою приватного DNS-сервера, а не загальнодоступного DNS-сервера.

5. Баланс навантаження - балансувальник навантаження надсилає запит до певного сервера веб-додатків у пулі серверів веб-додатків. Рішення приймається за допомогою випадкового або "кругового" алгоритму або іншого методу. Наприклад, він може вибрати сервер, який виконує найменшу кількість робіт (найменше навантаження). Якщо пакет пов'язаний з веб-сеансом, то балансування навантаження може направити повідомлення на сервер, який останнім часом обробляв запит в тому ж самому сеансі. Балансувачі навантаження можуть направляти запити, обробляючи складні правила, використовуючи системні та бізнес-політики, поточні та історичні показники, а також використання ресурсів і доступність у базових віртуальних машинах або системах.

6. Сервери веб-додатків - сервер веб-додатків повертає ресурс (зазвичай певну форму веб-контенту) на основі запиту користувача. На основі запиту веб-сервер отримує статичний вміст, звертаючись до файлової системи або викликає програму або службу для створення динамічного запитаного вмісту.

7. Перш ніж виконується будь-яка обробка, сервер веб-додатків може викликати Директорію користувачів для аутентифікації користувача і перевірки прав доступу для виконання запиту. Як правило, це робиться як частина процесу входу в систему, яка встановлює сеанс, який використовується для серії запитів.

8. Сервер веб-додатків визначає, чи може задовольняти запит локальним кешем і сховищем файлів. Якщо це так, відповідний вміст і пов'язані з ним дані повертаються користувачеві через брандмауер (див. 10). Якщо логіку програми необхідно викликати (сервером прикладних програм), то може знадобитися пошук даних з файлів, баз даних (див. 9), веб-сервісів, датчиків та інших джерел даних, а також програмне генерування нових даних або інформації..

9. Бази даних - серверу веб-застосунків може знадобитися доступ до бази даних для запиту деяких даних, щоб генерувати запитану відповідь.

10. Коли сервер веб-застосунків виконує свої завдання, отриманий вміст доставляється назад через брандмауер, який передає вміст у веб-переглядач користувача.

3.2 Дизайн системи

Розгортання компонентів для хостингу веб-додатків залежить від можливостей хмарних сервісів, які вибираються. DNS і CDN зазвичай живуть у загальнодоступній мережі - вони зазвичай купуються як послуги від відповідного постачальника. Для IaaS:

– Брандмауер і балансування навантаження розгортаються в хмарній службі. Багато постачальників хмарних сервісів мають доступ до послуг Firewall, або у вигляді спеціалізованих апаратних пристроїв, або у вигляді спеціалізованих систем, що працюють з відповідним програмним забезпеченням. Кілька надлишкових брандмауерів можуть бути розгорнуті, щоб уникнути однієї точки відмови, кожна з яких обробляє унікальну IP-адресу, де можуть використовуватися можливості DNS-серверів для відображення однієї URL-адреси на кілька IP-адрес. Баланс навантаження можна запускати на одному або декількох окремих серверах у хмарній службі, або він може працювати на тій же системі (системах), що і Firewall.

– Типово для серверів веб-застосунків використовується декілька екземплярів, всі вони обслуговують ті ж самі веб-сторінки. Це може бути як боротьба з очікуваною пропускною спроможністю запитів, так і забезпечення стійкості проти відмови одного примірника. Розташування примірників може

бути розглянуто, коли фізично віддалені екземпляри можуть допомогти вирішити проблеми, які впливають на один центр обробки даних.

– Каталог користувачів, кеш-пам'ять та сховище файлів виконуються у вигляді екземплярів віртуальних машин у службі IaaS, з резервуванням та переходом на відмову для кожного.

– Бази даних виконуються у вигляді віртуальних машин з декількома екземплярами та реплікаційними сховищами даних для цілей ємності та стійкості.

У випадку типової платформи PaaS, Firewall і Balancer навантаження є частиною платформи і просто вимагають конфігурації. Сервери веб-додатків також є частиною платформи - код програми повинен бути завантажений на них, але робота декількох екземплярів обробляється платформою, і все, що потрібно, це конфігурація числа та місця (ів) для використання. Аналогічно, PaaS зазвичай постачає базу даних як послугу, і загальноприйнятою для служби баз даних є забезпечення реплікації даних і масштабованість примірників.

Незалежно від того, де розгортаються компоненти - публічний, приватний або гібридний - необхідно розглянути та вирішити вимоги до життєвого циклу, операцій та управління. Там, де розгортаються компоненти, сильно впливатиме на те, як здійснюється управління та управління. Приватні розгортання можуть використовувати існуючі інструменти внутрішнього управління та управління, якщо вони мають доступ до хмарної інфраструктури. Для загальнодоступних, гібридних і зовнішніх розміщених приватних розгортань операції життєвого циклу - екземпляри, ініціювання, припинення - для компонентів поза брандмауером необхідно обговорити з приймаючими сторонами.

3.3 Хостинг веб-застосунку на Amazon Services

Веб-додаток - це будь-яке програмне забезпечення, доступ до якого здійснюється користувачами через веб-браузер або спеціалізований веб-клієнт. Зазвичай веб-програми структуровані на логічні рівні. Наприклад, загальна структура використовує три яруси. Перший рівень - це веб-браузер, який відповідає за представлення інтерфейсу користувача. Середній рівень - це сервер додатків, який відповідає за функціональність програми. Третій рівень - це сервер бази даних або файлова система, яка відповідає за зберігання даних.

Наступний підручник допомагає пройти процес розміщення масштабованого, надійного веб-додатка на інфраструктурі AWS. Ми розгорнемо зразок програми, демонструючи найкращі практики. До кінця цього підручника ми повинні мати можливість виконувати наступне:

– створіть віртуальний сервер, який називається екземпляром EC2, і використовуйте його як сервер додатків у хмарі.

– створити сервер бази даних, званий екземпляром БД.

– розгорніть зразок веб-програми на сервер додатків.

– налаштування масштабування та балансування навантаження для розподілу трафіку по мінімальному числу серверів додатків.

– пов'язуйте доменне ім'я з веб-програмою.

3.4 Архітектура системи

Перш ніж створювати та розгортати веб-додаток, ми повинні розробити нашу архітектуру, щоб гарантувати, що вона відповідає нашим вимогам. Наступна таблиця показує, як Amazon EC2, Amazon EBS, Amazon S3, автоматичне масштабування, еластичне балансування навантаження, Amazon CloudWatch, Amazon Route 53 і Amazon CloudFront працюють разом, щоб забезпечити бездоганну та економічну архітектуру.

Таблиця 3.1 - Відображення мінімальних вимог до архітектури системи Web App

Requirement	Solution
1	2
Недорогі, надійні сервери та бази даних	– Amazon EC2 надає віртуальні сервери в хмарі. Ми керуємо визначенням протоколів, портів і діапазонів вихідних IP-адрес, які можуть мати доступ до наших віртуальних серверів. – Amazon EBS надає постійну файлову систему для віртуальних серверів Amazon EC2. – Amazon RDS забезпечує рентабельний і змінюваний сервер баз даних, який легко адмініструвати.

Продовження табл.3.1

1	2
Простий спосіб надання серверів для обробки пікової потужності без витрат, коли додаткові потужності не потрібні	– Еластичне вирівнювання навантаження підтримує перевірку здоров'я на хостах, розподіляє трафік на віртуальні сервери в декількох ізольованих місцях, відомих як зони доступності, і динамічно додає або видаляє віртуальні сервери з обертанням балансування навантаження. – Автоматичне масштабування підтримує групи серверів, які можуть рости або зменшуватися за запитом. – CloudWatch збирає дані метрики для наших віртуальних серверів, які можна використовувати за допомогою автоматичного масштабування.
Надійний і економічно ефективний спосіб спрямовувати користувачів на веб-программу.	Amazon Route 53 відображає імена, що читаються людиною, до IP-адрес.

Наведена нижче схема показує приклад архітектури для веб-додатку, що використовує служби, описані в попередній таблиці. Рівні веб і додатків виконуються на екземплярах EC2 в публічних підмережах. Доступ до екземплярів EC2 над SSH контролюється групою безпеки, яка діє як брандмауер. Група автомасштабування підтримує парк екземплярів EC2, які можуть масштабуватися для обробки поточного навантаження. Ця група

автоматичного масштабування охоплює кілька зон доступності, щоб захистити від потенційної аварії однієї зони доступності. Балансування навантаження розподіляє трафік рівномірно між екземплярами EC2. Коли група автоматичного масштабування запускає або припиняє екземпляри на основі навантаження, балансувальник навантаження автоматично налаштовується відповідно. Рівень баз даних складається з екземплярів БД у приватних підмережах, включаючи основний і локальний підлеглий, розташований в декількох зонах доступності для захисту від відмови. Доступ до екземплярів БД з екземплярів EC2 контролюється групою безпеки. Amazon Route 53 забезпечує безпечну та надійну маршрутизацію нашого доменного імені до нашої інфраструктури, розміщеної на AWS.

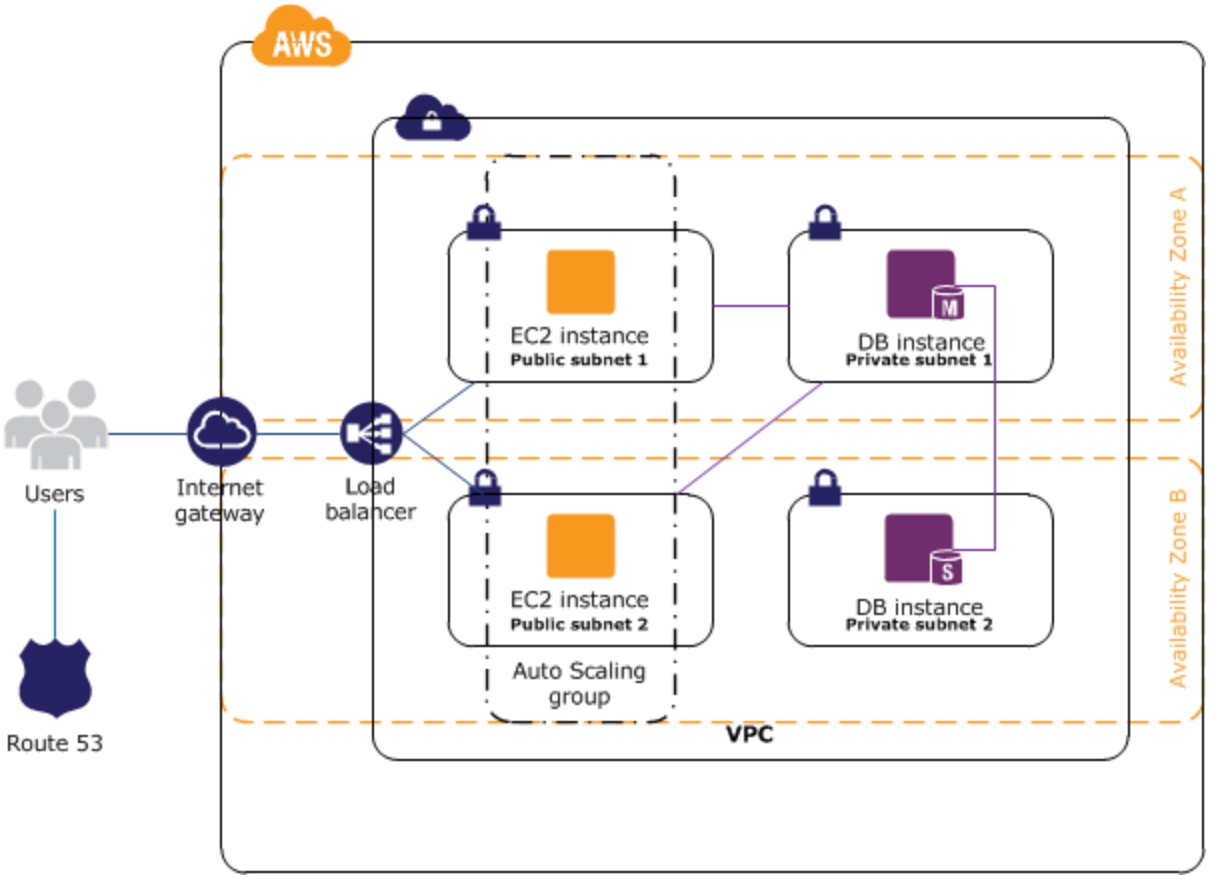


Рисунок 3.2 - Архітектура системи

3.5 Структура системи

У кеш-пам'яті додатків у пам'яті можна зменшити навантаження на служби та підвищити продуктивність і масштабованість рівня бази даних, кешуючи часто використовувану інформацію. Amazon ElastiCache [9] - це веб-сервіс, який дозволяє легко розгортати, керувати та масштабувати кеш-пам'ять у хмарі. Створений нами кеш-пам'ять може бути налаштований для автоматичного масштабування з завантаженням і для автоматичного заміщення невдалих вузлів. Amazon ElastiCache сумісний з протоколом Memcached, що спрощує міграцію з поточного локального рішення.

Конфігурація бази даних, резервне копіювання і відмовостійкість Багато веб-додатків містять певну форму стійкості, як правило, у формі реляційної або NoSQL бази даних. AWS пропонує як реляційну, так і інфраструктуру бази даних NoSQL. Крім того, ми можемо розгортати власне програмне забезпечення бази даних на екземплярі Amazon EC2.

Таблиця 4.2-Наступна таблиця підсумовує ці варіанти, які потім обговорюються більш детально.

	Рішення реляційних баз даних	Рішення NoSQL
Керована служба баз даних	Amazon Relational Database Service (RDS) – MySQL, Oracle, SQL Server	Amazon DynamoDB
Самоврядування	Хостинг реляційної СУБД на екземплярі Amazon EC2	Хостинг рішення NoSQL на екземплярі Amazon EC2

Служба реляційних баз даних Amazon (RDS)

Amazon RDS дає нам доступ до можливостей знайомого механізму бази даних MySQL, Oracle або Microsoft SQL Server. Код, програми та засоби, які ми вже використовуємо, можна використовувати з Amazon RDS. Amazon RDS

автоматично виправляє програмне забезпечення бази даних та створює резервні копії нашої бази даних, і зберігає резервні копії для певного періоду зберігання. Він також підтримує відновлення за часом. Ми отримуємо вигоду з гнучкості можливості масштабування ресурсів комп'ютера або можливостей зберігання, пов'язаних з нашим екземпляром реляційної бази даних, шляхом здійснення одного виклику API. Крім того, розгортання Amazon RDS Multi-AZ збільшує доступність бази даних і захищає нашу базу даних від незапланованих відключень. Репліки для читання Amazon RDS забезпечують копії веб-бази даних, доступних лише для читання, тому ми можемо розширювати можливості для розгортання баз даних з однією базою даних для важливих завантажень бази даних зчитування. Як і у всіх веб-службах Amazon, немає необхідних попередніх інвестицій, і ми платимо тільки за використані ресурси.

Хостинг реляційної бази даних (RDBMS) на екземплярі Amazon EC2

На додаток до керованої пропозиції Amazon RDS, ми можемо встановити наш вибір RDBMS (наприклад, MySQL, Oracle, SQL Server або DB2) на примірник EC2 і керувати ним самостійно. Клієнти AWS, які розміщують базу даних на Amazon EC2, успішно використовували різні моделі master / slave і replication, включаючи віддзеркалення для копій лише для читання та доставки журналу для завжди готових пасивних рабів.

Томи Amazon EBS автоматично забезпечують надмірність в зоні доступності, що збільшує їх доступність над простими дисками. Якщо продуктивність одного обсягу Amazon EBS не є достатнім для потреб наших баз даних, то можна збільшити обсяги для збільшення продуктивності IOPS для нашої бази даних. Для складних робочих навантажень ми також можемо використовувати EBS.

Рішення NoSQL

-Для підтримки реляційних баз даних AWS також пропонує Amazon DynamoDB, повністю керований сервіс баз даних NoSQL, що забезпечує

швидку та передбачувану продуктивність з безперервною масштабованістю. Використовуючи консоль керування AWS або API Amazon DynamoDB, ми можемо збільшувати або зменшувати потужність без простоїв або зниження продуктивності.

У хмарі AWS існує безліч варіантів зберігання, доступу та резервного копіювання даних та активів веб-додатків. Утиліта Amazon Simple Storage (Amazon S3) надає високодоступний і резервний сховище об'єктів. Amazon S3 є чудовим рішенням для зберігання об'єктів, що містять кілька статичних або повільних змін, таких як зображення, відео та інші статичні носії. Amazon S3 також підтримує кешування країв і потокове передавання цих ресурсів, взаємодіючи з послугою Amazon CloudFront. Для приєднаних файлових систем, таких як сховище, екземпляри EC2 можуть мати прикріплені томи Amazon Elastic Block Storage, які можуть діяти як диски для монтування для запуску екземплярів EC2. Amazon EBS відмінно підходить для даних, до яких потрібно звертатися як до блочного сховища, і що вимагає наполегливості за межами життя запущеного екземпляра, наприклад розділи бази даних і журнали програм.

4 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Проект орієнтований на хмарні обчислення, оскільки він став популярною парадигмою придбання та забезпечення інфраструктури обчислень, мереж та зберігання, що обіцяє еластичність попиту для масштабування та / або масштабування. Це, по суті, означає завантаження частин серверної кімнати організації до високоавтоматизованих комерційних центрів обробки даних. Крім величезного розвитку в підтримці технологій, таких як віртуалізація і утилізація, іншою ключовою причиною швидкого поглинання є підтримка авторитетних виробників, таких як Google, Yahoo і Amazon, які відомі тим, що мають надійні інфраструктури, які почали відкривати свої центри обробки даних для загального користування. Для перенесення IT-інфраструктури в технологію хмарних обчислень можуть бути декілька причин. наприклад, вартість в'їзду, зменшення ризику відмови IT-інфраструктури, підвищення рентабельності інвестицій, швидке реагування на зміни в попиті, швидке розгортання, підвищена безпека та можливість зосередитися на основній діяльності організації.

4.1 Файловий хостинг ownCLoud

У цьому проекті ми встановлюємо веб-додаток під назвою ownCLoud, використовуючи веб-сервер Amazon, який зберігатиме файли та папки з комп'ютера до хмари. Користувач завантажує матеріали через пряме посилання, створене з ownCLoud.

ownCloud на EC2 (Linux Micro) це програмна система для того, що зазвичай називають "файловим хостингом". Таким чином, ownCloud функціонально дуже схожий на широко використовуваний Dropbox, причому основна функціональна відмінність полягає в тому, що ownCloud є вільним і з відкритим вихідним кодом, і тим самим дозволяє будь-якому користувачеві встановлювати та експлуатувати його без заряду на приватному сервері, без обмежень на зберігання пробіл (за винятком ємності диска або квоти облікового запису) або кількості підключених клієнтів. Незважаючи на назву, система програмного забезпечення не використовує хмарну обчислювальну систему, якщо вона не налаштована вручну (наприклад, використання Swift сховища з балансуванням навантаження, наприклад).

Ось перші 5 кроків, необхідних для запуску першої інстанції:

4.1.1 Реєстрація для AWS

Щоб створити обліковий запис AWS:

1) відкрийте веб-сторінку http://aws.amazon.com/ і натисніть кнопку Зареєструватися.

2) дотримуйтесь інструкцій на екрані.

Частина процедури реєстрації передбачає отримання телефонного дзвінка та введення PIN-коду за допомогою клавіатури телефону.

Зверніть увагу на номер облікового запису AWS, тому що вам знадобиться для наступного завдання.

4.1.2 Створення користувача IAM

Служби в AWS, такі як Amazon EC2, вимагають надання облікових даних під час доступу до них, щоб служба могла визначити, чи маєте ви дозвіл на доступ до її ресурсів. Для консолі потрібен пароль.

Щоб створити групу адміністраторів необхідно:

1) увійдіть до консолі керування AWS і відкрийте консоль IAM за адресою https://console.aws.amazon.com/iam/;

2) у вікні навігації клацніть Групи, потім натисніть Створити нову групу;

3) у полі Ім'я групи введіть Адміністратори і натисніть кнопку Далі;

4) у списку політик встановіть прапорець поруч із політикою AdministratorAccess (за допомогою меню "Фільтр" і поля "Пошук" можна фільтрувати список політик);

5) натисніть кнопку Далі, а потім натисніть кнопку Створити групу.

Ваша нова група вказана під назвою "Група".

Щоб створити користувача IAM для себе, додайте користувача до групи адміністраторів і створіть пароль для користувача:

1) У вікні навігації клацніть Користувачі та натисніть кнопку Створити нових користувачів.

2) У полі 1 введіть ім'я користувача. Зніміть прапорець біля пункту Створити ключ доступу для кожного користувача, а потім натисніть кнопку Створити.

3) У списку користувачів натисніть назву (не прапорець) користувача, який ви тільки що створили. Можна скористатися полем пошуку для пошуку імені користувача.

4) У розділі Групи натисніть Додати користувача до груп.

5) Установіть прапорець біля групи "Адміністратори", а потім натисніть "Додати до груп".

6) Прокрутіть вниз до розділу "Документи безпеки". У розділі Облікові дані входу натисніть Керувати паролем.

7) Виберіть Призначити власний пароль, а потім введіть пароль у полях Пароль і Підтвердити пароль. Після завершення натисніть кнопку Застосувати.

Щоб увійти в систему як новий користувач IAM, вийдіть з консолі AWS, а потім скористайтеся наступною URL-адресою, де your_aws_account_id є номером вашого облікового запису AWS без дефісів (наприклад, якщо номер облікового запису AWS 1234-5678-9012, ваш AWS ID облікового запису - 123456789012):

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

Введіть щойно створене ім'я користувача та пароль IAM. Коли ви увійшли, відображається панель навігації "*your_user_name @ your_aws_account_id*".

Якщо ви не хочете, щоб URL для сторінки входу містив ваш ідентифікатор облікового запису AWS, можна створити псевдонім облікового запису. На інформаційній панелі IAM натисніть Налаштувати і введіть псевдонім, наприклад, назву вашої компанії. Щоб увійти після створення псевдоніма облікового запису, скористайтеся цією URL-адресою:

```
https://your_account_alias.signin.aws.amazon.com/console/
```

Щоб перевірити посилання для входу для користувачів IAM для вашого облікового запису, відкрийте консоль IAM і перевірте під посиланням для користувачів IAM на інформаційній панелі.

Докладніше про IAM див. IAM and Amazon EC2.

4.1.3 Створіть пару ключів

Щоб створити пару ключів необхідно виконати:

1) Увійдіть до AWS, використовуючи URL-адресу, створену в попередньому розділі. Відкрийте консоль Amazon EC2.

2) На панелі навігації виберіть регіон для пари ключів. Ви можете вибрати будь-який регіон, доступний для вас, незалежно від вашого місцезнаходження. Проте пари ключів є специфічними для регіону; наприклад, якщо ви плануєте запустити примірник у регіоні Західної (Орегонської) області США, потрібно створити пару ключів для екземпляра в регіоні Західна (Орегонська) область США.

3) Клацніть Key Pairs у вікні навігації.

4) Натисніть «Створити пару ключів».

5) Введіть назву нової пари ключів у полі "Ім'я пари" діалогового вікна "Створити пару ключів" і натисніть кнопку "Створити". Виберіть ім'я, яке легко запам'ятовується, наприклад ім'я користувача IAM, за яким слідує пара-клавіша, а також назва регіону. Наприклад, *me*-key-pair-*uswest2*.

6) Файл приватного ключа автоматично завантажується вашим браузером. Ім'я базового файлу - це ім'я, вказане як назва пари ключів, а розширення імені файлу - .pem. Збережіть файл закритого ключа в безпечному місці.

Це єдиний шанс зберегти файл закритого ключа. Під час запуску екземпляра та відповідного закритого ключа кожен раз, коли ви підключаєтеся до екземпляра, потрібно вказати ім'я пари ключів.

Якщо ви використовуєте клієнт SSH на комп'ютері Mac або Linux для підключення до екземпляра Linux, скористайтеся наведеною нижче командою, щоб встановити права доступу до файлу приватного ключа, щоб тільки ви могли його прочитати.

```
$ chmod 400 your_user_name-key-pair-region_name.pem
```

Для отримання додаткової інформації див. Amazon EC2 Key Pairs.

Щоб підключитися до свого примірника за допомогою пари ключів

У вашому екземплярі Linux з комп'ютера, на якому запущено Mac або Linux, ви вкажете файл .pem на ваш SSH-клієнт за допомогою параметра -i і шлях до вашого закритого ключа. Щоб підключитися до екземпляра Linux з комп'ютера під керуванням Windows, можна використовувати або MindTerm, або PuTTY. Якщо ви плануєте використовувати PuTTY, вам доведеться встановити його та використовувати наступну процедуру для перетворення файлу .pemfile у файл .ppk.

(Optional) To prepare to connect to a Linux instance from Windows using PuTTY

Завантажте та встановіть з http://www.chiark.greenend.org.uk/~sgtatham/putty/.

Обов'язково встановіть весь пакет!

1) Запустіть PuTTYgen (наприклад, у меню "Пуск" натисніть Усі програми> PuTTY> PuTTYgen).
2) У розділі Тип ключа, щоб створити, виберіть SSH-2 RSA.

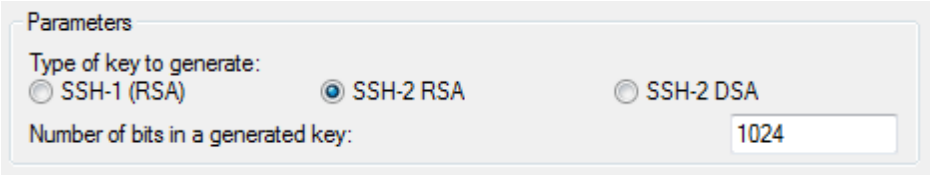


Рисунок 4.1 – Вибір типу ключа

3) Натисніть кнопку Завантажити. За замовчуванням PuTTYgen відображає лише файли з розширенням .ppk. Щоб знайти файл .pem, виберіть параметр для відображення файлів усіх типів.

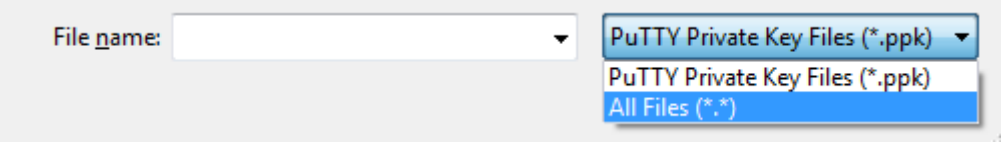


Рисунок 4.2 завантаження файлу

4) Виберіть файл приватного ключа, створений у попередній процедурі, і натисніть кнопку Відкрити. Натисніть OK, щоб відхилити діалогове вікно підтвердження.
5) Натисніть Зберегти закритий ключ. PuTTYgen відображає попередження про збереження ключа без фрази. Натисніть кнопку Так.
6) Вкажіть однакову назву для ключа, який використовувався для пари ключів. PuTTY автоматично додає розширення .ppk.

4.1.4 Створити віртуальну приватну хмару (VPC)

Amazon VPC дозволяє запускати ресурси AWS у віртуальну мережу, яку ви визначили. Якщо у вас є VPC за замовчуванням, ви можете пропустити цей розділ і перейти до наступного завдання, Створити группу безпеки. Щоб визначити, чи є у вас VPC за замовчуванням, див. Підтримувані платформи в консолі Amazon EC2. В іншому випадку ви можете створити VPC у своєму обліковому записі за умовчанням, виконавши наведені нижче дії.

Якщо ваш обліковий запис підтримує EC2-Classic в регіоні, у вас немає стандартної VPC у цьому регіоні. Примірники T2 повинні бути запущені в VPC.

Щоб створити VPC за умовчанням:

1) відкрийте консоль Amazon VPC у https://console.aws.amazon.com/vpc/;

2) на панелі навігації виберіть регіон для VPC. VPC є специфічними для регіону, тому ви повинні вибрати той самий регіон, в якому була створена пара ключів;

3) на інформаційній панелі VPC натисніть Запустити майстра VPC;

4) На кроці 1: виберіть сторінку конфігурації VPC, переконайтеся, що вибрано VPC з єдиною загальною підмережею, і натисніть кнопку Вибрати;

5) На кроці 2: VPC з єдиною сторінкою загальної підмережі введіть дружнє ім'я для вашого VPC в полі імені VPC. Залиште інші налаштування конфігурації за замовчуванням і натиснітьСтворити VPC. На сторінці підтвердження натисніть кнопку OK.

4.1.5 Створити групу безпеки

Групи безпеки діють як брандмауер для відповідних екземплярів, контролюючи як вхідний, так і вихідний трафік на рівні екземпляра. Ви повинні додати правила до групи безпеки, які дозволяють підключатися до вашого примірника з IP-адреси за допомогою SSH. Можна також додати правила, які дозволяють вхідний і вихідний доступ HTTP і HTTPS з будь-якого місця.

Щоб створити групу безпеки з мінімальними привілеями

1) відкрийте консоль Amazon EC2;

2) на панелі навігації виберіть регіон для групи безпеки. Групи захисту відносяться до регіону, тому ви повинні вибрати той самий регіон, в якому була створена пара ключів;

3) у вікні навігації клацніть Security Groups;

4) натисніть Створити групу безпеки;

5) введіть назву нової групи безпеки та опис. Виберіть ім'я, яке легко запам'ятати, наприклад ім'я користувача IAM, а потім _SG_, а також назву регіону. Наприклад, *me*_SG_*uswest2*;

6) у списку VPC виберіть VPC. Якщо у вас є VPC за замовчуванням, це те, що позначено зірочкою (*).

Примітка

Якщо ваш обліковий запис підтримує EC2-Classic, виберіть VPC, створену в попередньому завданні.

На вкладці Вхідні створіть наступні правила (натисніть кнопку Додати правило для кожного нового правила) і натисніть кнопку Створити:

– виберіть HTTP у списку Тип і переконайтеся, що для джерела встановлено значення Anywhere (0.0.0.0/0);

– виберіть HTTPS зі списку Тип і переконайтеся, що для джерела встановлено значення Anywhere (0.0.0.0/0);

– виберіть SSH у списку Тип. Переконайтеся, що в полі Source (Джерело) вибрано Custom IP (Персональний IP-адрес) і вкажіть загальнодоступну IP-адресу комп'ютера або мережі в нотації CIDR. Щоб вказати окрему IP-адресу в позначенні CIDR, додайте префікс маршрутизації / 32. Наприклад, якщо ваша IP-адреса 203.0.113.25, вкажіть 203.0.113.25/32. Якщо ваша компанія виділяє адреси з діапазону, вкажіть весь діапазон, наприклад 203.0.113.0/24.

З міркувань безпеки ми не рекомендуємо дозволяти доступ SSH з усіх IP-адрес (0.0.0.0/0) до вашого екземпляра, за винятком цілей тестування і лише протягом короткого часу.

Після налаштування та встановлення Putty ми будемо підключені до віддаленого комп'ютера в хмарі, використовуючи нашу унікальну пару ключів. Коли ми підключені, ми можемо встановити веб-додаток ownCloud на Amazon Linux.

ownCLoud — це програма з відкритим вихідним кодом, що дозволяє синхронізувати особисті дані (контакти, календарі, закладки, фотографії) з різних пристроїв (настільних, планшетних, телефонних). Деякі базові знання з Linux, мереж і комп'ютерної безпеки необхідні тут, але якщо ці інструкції дотримуються уважно, не потрібно вимагати виправлення неполадок. Це обговорення передбачає використання AWS, а особливо Amazon Linux AMI, але будь-якої кількості сучасних установок Linux достатньо. Однак, оскільки у світі з відкритим вихідним кодом є багато варіантів, ваш пробіг може змінюватись залежно від обраної версії й дистрибутиву Linux. Відомо, що ці інструкції працюють з представленими ресурсами. Щоб тримати речі передбачуваними, ця дискусія передбачає, що ваш екземпляр EC2 буде використовуватися виключно для ownCloud. І, нарешті, діапазон функцій, продемонстрований тут, буде обмежений лише можливостями контакту та календаря.

ownCloud надає доступ до наших даних через веб-інтерфейс або WebDAV, надаючи платформу для перегляду, синхронізації та спільного використання пристроїв легко - все під вашим контролем. Відкрита архітектура ownCloud розширюється за допомогою простого, але поганого API для додатків і плагінів і працює з будь-яким сховищем.

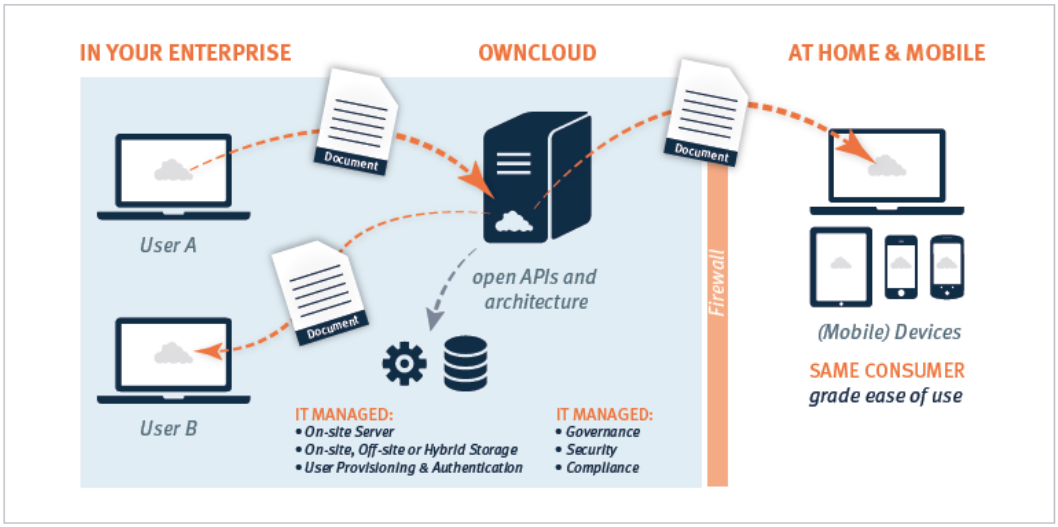


Рисунок 4.3 – Можливості ownCloud з синхронізації даних

4.2 Огляд архітектури ownCloud

У виробництві, ownCloud найчастіше розгортається як n-tier навантаження збалансований веб-додаток, що працює в дата-центр або керованої інфраструктури хмара. ownCloud може бути розгорнутий на фізичних, віртуальних або приватних хмарних серверах з використанням власних бінарних файлів або віртуального пристрою. Завжди є балансування навантаження на передньому кінці розгортання, підключене щонайменше до двох веб-серверів. Веб-сервери ownC¬loud розміщують PHP-код і найчастіше розгортаються на Apache через Linux, хоча IIS і Apache на Windows також підтримуються. Потім всі веб-сервери підключаються до бази даних (часто кластерний екземпляр бази даних MySQL) для користувацької інформації, включаючи кешовані файли, метадані користувачів і груп, списки спільних файлів і сховища, необхідні для дозволених власних програм. Веб-сервери також підключені до спільної базової пам'яті, часто кластерної файлової системи. Завдяки цій конфігурації ownCloud можна легко масштабувати, щоб задовольнити вимоги до навантаження, забезпечуючи при цьому всі необхідні резервні і резервні вимоги для досягнення цілей доступності системи.

4.3 Створення програми ownCloud

4.3.1 Конфігурація Apache

Скопіюйте файл конфігурації Apache до каталогу конфігурації:

```
# cp /etc/webapps/owncloud/apache.example.conf
/etc/httpd/conf/extra/owncloud.conf
```

І включити його внизу /etc/httpd/conf/httpd.conf:

```
Include conf/extra/owncloud.conf
```

Активувати php (встановити пакет php-apache):

```
LoadModule php5_module modules/libphp5.so
Include conf/extra/php5_module.conf
```

Переконайтеся, що веб-сервер може записувати до каталогу ownCloud:

```
# chown -R http:http /usr/share/webapps/owncloud/
```

Відкрийте http://localhost/ у веб-переглядачі. Тепер ви повинні мати можливість створити обліковий запис користувача та дотримуватися майстра інсталяції.

4.3.2 Доступ до веб-інтерфейсу ownCloud

Щоб отримати доступ до веб-інтерфейсу ownCloud:

1) Введіть URL-адресу сервера ownCloud у навігаційну панель браузера. Відкриється вікно реєстрації ownCloud.

Рисунок 4.4- вікно реєстрації ownCloud

2) Введіть дійсне ім'я користувача та пароль. Комбінація імені користувача та пароля може бути такою, яку ви самі налаштували під час створення вашого сервера власного сервера, або тих, які надаються вашою компанією або постачальником послуг. Якщо ви налаштували сервер самостійно або керуєте сервером, можна додати додаткових користувачів, налаштувавши серверний сервер

3) Натисніть кнопку Увійти. Відкриється головний інтерфейс ownCloud.

Рисунок 4.5- Основний користувальницький інтерфейс ownCloud

4.3.3 Спільне використання файлів локально

Якщо цей параметр увімкнено адміністратором, ви можете обмінюватися файлами або папками на ownCloud з локальним користувачем, групою або будь-якою особою в Інтернеті за допомогою загального посилання. Спільні файли та папки позначаються значком поділу трикутної форми та статусом Спільний у файлі або рядку папок.

Щоб створити локальний доступ до інших користувачів або груп на сервері ownCloud:

1. Наведіть курсор на елемент на сторінці "Файли"

2. Натисніть піктограму Share (Діалогове вікно) Відкриється діалогове вікно Share (Спільний доступ), у якому відображаються наступні параметри: Введіть ім'я користувача або групи, з якою ви хочете поділитися. Якщо ви хочете поділитися з більш ніж одним, потрібно створити кожну папку окремо. Перевірте дозволи, які потрібно мати користувачеві або групі, і, за бажанням, надішліть їм повідомлення електронною поштою.

4.3.4 Перевірка власного додаткаCloud на веб-сторінці

Щоб побачити додаток ownCloud, який дозволяє користувачеві завантажувати матеріали, ми створили зразок веб-сторінки *http://nurebooks.weebly.com* . На цьому веб-сайті користувач може завантажити файли і папки, які спільно використовуються за допомогою посилання через ownCloud.

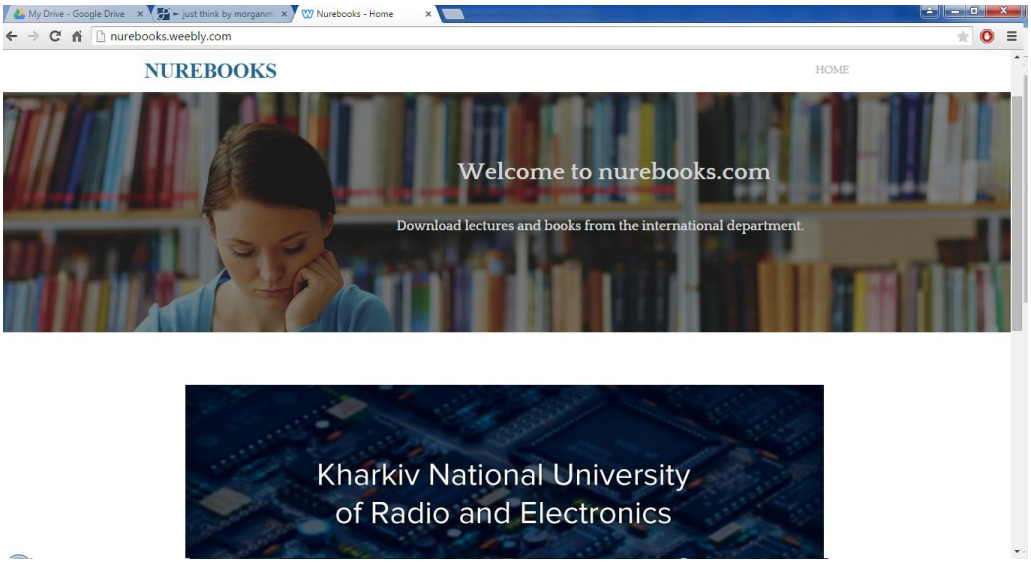


Рисунок 4.6- Тестування інтерфейсу веб-сторінки для завантаження файлів

Після того як ми відкриємо нашу веб-сторінку, ми бачимо кілька варіантів для користувача, щоб завантажити будь-який вміст, який вони потребують.

Рисунок 4.7- Коли користувач вибирає тему, яка підкреслена прямим кліком

Обрана тема підкреслена під час переміщення курсору до неї. Після цього користувач може завантажити загальний файл або папку з веб-сторінки.

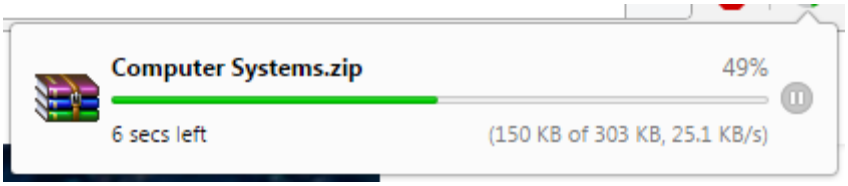


Рисунок 4.8- Завантаження вмісту

Таким чином, адміністратор може ділитися будь-якими файлами та папками, зображеннями, документами, посиланнями та музикою тощо з будь-якої області, збереженої в додатку ownCloud. Вносити зміни, коли і коли-небудь, використовуючи Amazon Linux через хмару. Таким чином, користувач може завантажити матеріали з веб-сторінки з будь-якої частини світу. Оскільки ownCLoud є відкритим вихідним кодом, будь-який інший користувач може також завантажувати та спільно використовувати документи.

5 ОХОРОНА ПРАЦІ

5.1 Аналіз потенційних небезпечних і шкідливих виробничих чинників проектованого об’єкту, що мають вплив на персонал

У даному дипломному проекті розробляється програмне забезпечення.

Розроблене програмне забезпечення орієнтоване на роботу з персональним комп'ютером. Експлуатовані для вирішення внутрішньовиробничих завдань ПЕОМ типу IBM PC мають наступні характеристики:

споживана потужність	220 Вт;
робоча напруга	220 В;
напруга джерел живлення	+12 В; - 12 В; +5 В;
робоча частота	50 Гц.

Відповідно до ДСН 3.3.6.042-99 [21] до легкої фізичної роботи відносяться всі види діяльності, виконувані сидячи і ті, що не потребують фізичної напруги. Робота користувача ПК відноситься до категорії 1а.

При роботі на ПЕОМ користувач піддається ряду потенційних небезпек. Унаслідок недотримання правил техніки безпеки при роботі з машиною (невиконання огляду відкритих частин ПЕОМ, що знаходяться під напругою або знятих для ремонту вузлів) для користувача існує небезпека поразки електричним струмом.

Джерелами підвищеної небезпеки можуть служити наступні елементи:

- розподільний щит;
- джерела живлення;
- блоки ПЕОМ і друку, що знаходяться в ремонті.

Ще одна проблема полягає у тому, що спектр випромінювання комп'ютерного монітора включає рентгенівську, ультрафіолетову і інфрачервону області, а також широкий діапазон хвиль інших частот. Небезпека рентгенівського проміння мала, оскільки цей вид випромінювання поглинається речовиною екрану. Проте велику увагу слід приділяти біологічним ефектам низькочастотних електромагнітних полів (аж до порушення ДНК).

Відповідно до ДСанПІН 3.3.2.007-98 [22], при обслуговуванні ПЕОМ мають місце фізичні і психофізичні небезпечні, а також шкідливі виробничі чинники:

- підвищене значення напруги в електричному ланцюзі, замикання
- якої може відбутися через тіло людини;
- підвищений рівень статичної електрики;
- підвищений рівень електромагнітних випромінювань;
- підвищена або знижена температура повітря робочої зони;
- підвищений або знижений рух повітря;
- підвищена або знижена вологість повітря;
- відсутність або недостатність природного світла;
- підвищена пульсація світлового потоку;
- недостатня освітленість робочого місця;
- підвищений рівень шуму на робочому місці;
- розумове перенапруження;
- емоційні навантаження;
- монотонність праці.

5.2 Заходи щодо техніки безпеки

Основним небезпечним чинником при роботі з ЕОМ є небезпека поразки людини електричним струмом, яка посилюється тим, що органи чуття людини не можуть на відстані знайти наявності електричної напруги на устаткуванні.

Проходячи через тіло людини, електричний струм чинить на нього складну дію, що є сукупністю термічної (нагрів тканин і біологічних середовищ), електролітичної (розкладання крові і плазми) і біологічної (роздратування і збудження нервових волокон і інших органів тканин організму) дій.

Тяжкість поразки людини електричним струмом залежить від цілого ряду чинників:

– значення сили струму;

– електричного опору тіла людини і тривалості протікання через нього струму;

– роду і частоти струму;

– індивідуальних властивостей людини і навколишнього середовища.

Розроблений дипломний проект передбачає наступні технічні способи і засоби, що застерігають людину від ураження електричним струмом [23]:

– заземлення електроустановок;

– занулення;

– захисне відключення;

– електричне розділення ятерів;

– використовування малої напруги;

– ізоляція частин, що проводять струм;

– огорожа електроустановок.

Занулення зменшує напругу дотику і обмежує година, протягом якого людина, ткнувшись до корпусу, може потрапити під дію напруги.

Струм однофазного короткого замикання визначається по наближеній формулі:

$$I_K = \frac{\text{Uф}}{\text{Zп} + \frac{\text{Zт}}{3}}\ , \qquad (5.1)$$

де Uф - номінальна фазна напруга мережі, В;

Zп - повний опір петлі, створене фазними і нульовими дротами, Ом;

Z_T - повний опір струму короткого замикання на корпус, Ом.

Згідно таблиці 4 [24]: $Z_T/3 = 0{,}1$ Ом.

Для провідників і жил кабелю для розрахунку повного опору петлі використовуємо формулу(5.2.) :

$$\text{Zп} = \sqrt{\text{Rп}^2 + \text{Xп}^2}\ , \qquad (5.2)$$

де Rп = Rф + Ro - сумарний активний опір фазного Rф і нульового Ro дротів, Ом;

Xп - індуктивний опір паяння дротів, Ом.

Перетин 1 км мідного дроту S = 2.5 мм, тоді згідно таблицям 5 і 6 [24], має такий опір:

Xп = 0,11 Ом;

Rф = 7,55 Ом;

Ro = 7,55 Ом.

Отже, Rп = 7,55 + 7,55 = 15,1 Ом.

Тоді по формулі(5.2) знаходимо повний опір петлі :

$$Zп = \sqrt{15,1^2 + 0,11^2} \approx 15,1 (Ом).$$

Струм однофазного короткого замикання рівний:

$$Iк = \frac{220}{15,1 + 0,1} = 14,47 \ (А).$$

Дія плавкої вставки на ПЕОМ забезпечується, якщо виконується співвідношення:

$$Iк \geq k * Iн, \qquad (5.3)$$

де Iн - номінальний струм спрацьовування плавкої вставки, А;

k - коефіцієнт кратності нелінійного струму Iн, А.

Коефіцієнт кратності нелінійного струму Iн розраховується по формулі(5.4.) :

$$Iн = P / U, \qquad (5.4)$$

де P = 220 Вт - споживана потужність;

U = 220 В - робоча напруга;

k = 3 А - для плавких вставок.

Отже, Iн = 220 / 220 = 1 А.

Підставивши значення у вираз(5.3), одержимо:

14,47> 3*1.

Таким чином, доведено, що апарат забезпечить спрацьовування (і захист) при підвищенні номінального струму.

5.3 Заходи, що забезпечують виробничу санітарію і гігієну праці

Вимоги до виробничих приміщень встановлюються *ДСП 173-96* [25], СНіП, відповідними ГОСТами і ОСТамі з урахуванням небезпечних і шкідливих чинників, що утворюються в процесі експлуатації електроустаткування.

Підвищення працездатності людини і збереження її здоров'я забезпечується стабільними метеорологічними умовами. Мікроклімат виробничих приміщень [21] визначається діючими на організм людини поєднаннями температури, вологості і швидкості руху повітря, а також температури навколишніх поверхонь. Значне коливання параметрів мікроклімату приводити до порушення систем кровообігу, нервової і потовидільної, що може викликати підвищення або пониження температури тіла, слабкість, запаморочення і навіть непритомність.

Відповідно до ДСН 3.3.6.042-99 [21] встановлюють оптимальну і допустиму температуру, відносну вологість і швидкість руху повітря в робочій зоні . За відсутності надмірного тепла, вологи, шкідливих речовин в приміщенні досить природної вентиляції.

У приміщенні для виконання робіт операторського типу (категорія 1а), пов'язаних з нервово-емоційною напругою, проектом передбачається дотримання наступних нормованих величин параметрів мікроклімату (табл. 5.1).

Таблиця 5.1 - Санітарні норми мікроклімату робочої зони приміщень для робіт категорії 1а.

Пора року	Температура, С	Відносна вологість, %	Швидкість руху повітря, м/с
Холодна	22…24	40…60	0,1
Тепло	23…25	40…60	0,1

У приміщенні, де знаходиться ПЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції (з пристроєм вентиляційних каналів в перекриттях будівлі і вертикальних шахт) й установленого промислового кондиціонера фірми Mitsubishi, який дозволяє вирішити переважну більшість завдань по створенню та підтримці необхідних параметрів повітряного середовища. Цей метод забезпечує приток потрібної кількості свіжого повітря, визначеного в СНіП (30 $м^3$ в годину на одного працівника).

Шум на виробництві має шкідливу дію на організм людини. Стомлення операторів через шум збільшує число помилок при роботі, призводить до виникнення травм. Для оператора ПЕОМ джерелом шуму є робота принтера. Щоб усунути це джерело шуму, використовують наступні методи. При покупці принтера слід вибирати найбільш шумозахисні матричні принтери або з великою швидкістю роботи (струменеві, лазерні). Рекомендується принтер поміщати в найбільш віддалене місце від персоналу, або застосувати звукоізоляцію та звукопоглинання (під принтер підкладають демпфуючі підкладки з пористих звукопоглинальних матеріалів з листів тонкої повсті, поролону, пеноплену).

При роботі на ПЕОМ, проектом передбачені наступні методи захисту від електромагнітного випромінювання: обмеження часом, відстанню, властивостями екрану.

Обмеження годині роботи на ПЕОМ складає 3,5-4,5 години. Захист відстанню передбачає розміщення монітора на відстані 0,4-0,5 м від оператора. Передбачений монітор 20" TFT, Samsung 2043BW відповідає вимогам стандарту [26].

Стандарт [26] пред’являє жорсткі вимоги в таких областях: ергономіка (фізична, візуальна і зручність користування), енергія, випромінювання(електричних і магнітних полів), навколишнє середовище і екологія, а також пожежна та електрична безпека, які відповідають всім вимогам ДСанПІН 3.3.2.007-98 [22].

Для зниження стомлюваності та підвищення продуктивності праці обслуговуючого персоналу в колірній композиції інтер'єру приміщень для ПЕОМ дипломним проектом пропонується використовувати спокійні колірні поєднання і покриття, що не дають відблисків.

У проекті передбачається використання сумісного освітлення. У світлий час доби приміщення освітлюватиметься через віконні отвори, в решту часу використовуватиметься штучне освітлення.

Як штучне освітлення необхідно використовувати штучне робоче загальне освітлення. Для загального освітлення необхідно використовувати люмінесцентні лампи. Вони володіють наступними перевагами: високою світловою віддачею, тривалим терміном служби, хоча мають і недоліки: високу пульсацію світлового потоку.

При експлуатації ПЕОМ виробляється зорова робота. Відповідно до ДБН В.2.5-28:2018 [27] ця робота відноситься до розряду 5а. При цьому нормоване освітлення на робочому місці(Ен) при загальному освітленні дорівнює 200 лк.

Приміщення завдовжки 12 м, шириною 10 м, заввишки 4 м обладнується світильниками типу ЛП02П, оснащеними лампами типу ЛБ зі світловим потоком 3120 лм кожна.

Виконаємо розрахунок кількості світильників в робочому приміщенні завдовжки a=12 м, шириною b=10 м, заввишки з=4 м, використовуючи формулу (5.5) розрахунку штучного освітлення при горизонтальній робочій поверхні методом світлового потоку:

$$n = (E \cdot S \cdot Z \cdot k)/(F \cdot U \cdot M), \quad (5.5)$$

де F - світловий потік = 3120 лм;

E - максимально допустима освітленість робочих поверхонь = 200 лк;

S - площа підлоги = 120 м2;

Z - поправочний коефіцієнт світильника = 1,2;

k - коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації світильників = 1,5;

n - кількість світильників;

U - коефіцієнт використовування освітлювальної установки = 0,6;

M - кількість ламп у світильнику =2.

З формули (5.5) виразимо n (5.6) і визначимо кількість світильників для даного приміщення:

$$n = (E \cdot S \cdot Z \cdot k)/(F \cdot U \cdot M), \quad (5.6)$$

Отже, $n = (200 \cdot 120 \cdot 1,2 \cdot 1,5)/(3120 \cdot 0,6 \cdot 2) = 12$

Виходячи з цього, рекомендується використовувати 12 світильників. Світильники слід розміщувати рядами, бажано паралельно стіні з вікнами. Схема розташування світильників зображена на рис. 5.1.

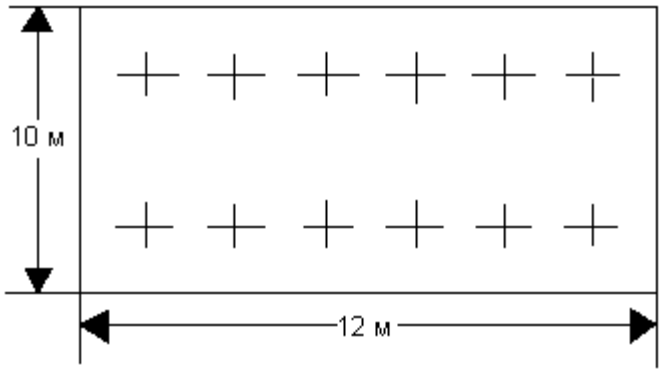


Рисунок 5.1 - Схема розташування світильників

5.4 Рекомендації по пожежній безпеці

Пожежі в приміщеннях, де встановлена обчислювальна техніка, представляють небезпеку для життя людини. Пожежі також пов’язані як з матеріальними втратами, так і з відмовою засобів обчислювальної техніки, що у свою чергу спричиняє за собою порушення ходу технологічного процесу.

Пожежа може виникнути при наявності горючої речовини та внесення джерела запалювання в горюче середовище. Пальними матеріалами в приміщеннях, де розташовані ПЕОМ, є:

– поліамід - матеріал корпусу мікросхеми, горюча речовина, температура самозаймання аерогелю 420 З ;

– полівінілхлорид - ізоляційний матеріал, горюча речовина, температуразапалювання 335 З, температура самозаймання 530 З, кількість енергії, що виділяється при згоранні - 18000 - 20700 кДж/кг;

– стеклотекстоліт ДЦ - матеріал друкарських плат, важкозаймистий матеріал, показник горючості 1.74, не схильний до температурного самозаймання;

– пластика кабельний №489 - матеріал ізоляції кабелю, горючий матеріал, показник горючості більш 2.1;

– деревина - будівельний і обробний матеріал, матеріал з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, теплота згорання 18731 - 20853 кДж/кг, температура запалювання 399 З, схильна до самозаймання [24].

Згідно ДСТУ Б В.1.1-36:2016 [28] приміщення відносяться до категорії В (пожежовибухонебезпечним) і згідно правилам побудови електроустановок простір усередині приміщення відноситься до вогненебезпечної зони класу П - IIа (зони, розташовані в приміщеннях, в яких зберігаються тверді горючі речовини).

Потенційними джерелами запалення при роботі ПЕОМ є:

– іскри при замиканні і розмиканні ланцюгів;

– іскри і дуги коротких замикань;

– перегріви від тривалого перевантаження і наявності перехідного опору.

Продуктами згорання, що виділяються при пожежі, є: оксид вуглецю, сірчистий газ, оксид азоту, синильна кислота, акропеін, фосген, хлор та ін. При горінні пластмас, окрім звичайних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідрідні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол та ін., що шкідливо впливають на організм людини.

Для захисту персоналу від дії небезпечних і шкідливих чинників пожежі проектом передбачається застосування промислового протигаза з коробкою марки В (жовта).

Пожежна безпека об’єктів народного господарства регламентується ГОСТ 12.1.004-91 [29] і забезпечується системами запобігання пожежам і протипожежному захисту. Для успішного гасіння пожеж вирішальне значення

має швидке виявлення пожежі і своєчасний виклик пожежних підрозділів до місця пожежі.

Зменшити горюче навантаження не представляється можливим, тому проектом передбачається застосувати наступні способи і їх комбінації для запобігання утворенню(внесення) джерел запалення :

– застосування устаткування, що задовольняє вимогам електростатичної безпеки;

– застосування в конструкції швидкодіючих засобів захисного відключення можливих джерел запалення;

– виключення можливості появи іскрового заряду статичної електрики в горючому середовищі з енергією, рівної і вище мінімальної енергії запалення;

– підтримка температури нагріву поверхні машин, механізмів, устаткування, пристроїв, речовин і матеріалів, які можуть увійти до контакту з пальним середовищем, нижче гранично допустимої, становить 80% якнайменшої температури самозаймання пального.

– заміна небезпечних технологічних операцій більш безпечними;

– ізольоване розташування небезпечних технологічних установок і устаткування;

– зменшення кількості пальних і вибухонебезпечних речовин, що знаходяться у виробничих приміщеннях;

– запобігання можливості утворення пальних сумішей на лінії, вентиляційних системах і ін.;

– механізація, автоматизація та справність(потокова) виробництва;

– суворе дотримання стандартів і точне виконання встановленого технологічного режиму;

– запобігання можливості появи в небезпечних місцях джерел запалення;

– запобігання розповсюдженню пожеж і вибухів;

– використовування устаткування і пристроїв, при роботі яких не виникає джерел запалення;

– виконання вимог сумісного зберігання речовин і матеріалів;

– наявність громовідводу;

– організація автоматичного контролю параметрів, що визначають джерела запалення;

– ліквідація можливості самозаймання речовин і матеріалів.

Для запобігання пожежі в обчислювальних центрах проектом пропонується виконання наступних вимог:

– електроживлення ЕОМ повинно мати автоматичне блокування відключення електроенергії на випадок зупинки системи охолоджування і кондиціонування;

– система вентиляції обчислювальних центрів повинна бути обладнана блокуючими пристроями, що забезпечують її відключення на випадок пожежі;

– робочі місця повинні бути оснащені пожежними щитами, сигналізацією, засобами для сповіщення про пожежну небезпеку (телефонами), медичними аптечками для надання першої медичної допомоги, розробленим планом евакуації.

Для зниження пожежної небезпеки в приміщеннях використовуються первинні засоби гасіння пожеж, а також система автоматичної пожежної сигналізації, яка дозволяє знайти початкову стадію загоряння, швидко і точно оповістити службу пожежної охорони про час і місце виникнення пожежі.

Відповідно до НАПБ А.01.001-2014 [30] приміщення категорії В підлягають устаткуванню системами автоматичної пожежної сигналізації. Проектом передбачається застосування датчика типу ІДФ - 1(димовий фотоелектричний датчик), оскільки специфікою пожеж обчислювальної техніки

і радіоапаратури є, в першу чергу, виділення диму, а потім - підвищення температури.

При виникненні пожежі в робочому приміщенні обслуговуючий персонал зобов'язаний негайно вжити заходи по ліквідації пожежі. Для ліквідації пожежі використовують вогнегасники (хімічно-пінні, пінні для повітря ОП-5, ОП-6, ОП-9, вуглекислотні ОУ-5), пісок, пожежний інвентар(сокири, ломи, багри, шерстяну або азбестову ковдри) [31]. Як засіб індивідуального захисту проектом передбачається використовування промислового протигаза з маскою, фільтруючої коробки В.

В якості організаційно-технічних заходів рекомендується проводити навчання робочого персоналу правилам пожежної безпеки.

ВИСНОВКИ

Парадигма Cloud Computing - це новий підхід до вирішення старих проблем. Ця парадигма пропонує багато переваг підприємствам, галузям і університетам. Багато великих ІТ-компаній розробляють нові хмарні додатки та створюють нову хмарну інфраструктуру. Більшість досліджень у літературі зосереджувалася на перевагах, можливостях, перевагах, недоліках, ризиках та конфігурації хмарних обчислень для підприємств.

В дипломній роботі ми намагалися показати, що Cloud Computing також можна використовувати для університетів. Використання хмарних обчислень у університетах має багато переваг, таких як доступ до сховищ файлів, електронних листів, баз даних, освітніх ресурсів, дослідницьких додатків і інструментів де-небудь для викладачів, адміністраторів, персоналу, студентів та інших користувачів університету, за вимогою. Кілька університетів вже розпочали технологію хмарних обчислень для освітнього використання. Основною метою запропонованого прототипу є; ефективне управління технологічними потребами університетів, таких як постачання програмного забезпечення, забезпечення платформи розробки, зберігання даних і обчислень.

Під час виконання розділу «Охорона праці» було проаналізовано умови праці, виявлені причини травматизму і захворювань, можливі небезпечні й шкідливі виробничі фактори. Також було проведено ряд розрахунків щодо виконання вимог охорони праці в приміщенні відділу програмного забезпечення. Дотримання цих вимог є важливим для збереження працездатності та здоров’я працівників.

СПИСОК ДЖЕРЕЛ ПОСИЛАНЬ

1) I. Foster, The grid: Computing without bounds, Scientific American, vol. 288, No. 4, (April 2003), pp. 7885.

2) R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 25:599616, 2009.

3) The Transformation of Education through State Education Clouds, www.ibm.com/ibm/files/N734393J24929X18/EBW0 3002-USEN-00.pdf

4) Behrend,T.S., Wiebe,E.N., London,J.E., and Johnson,E.C. (2011). Cloud computing adoption and usage in community colleges. Behavior & Information Technology, 30 (2), 231–240.

5) Dan R.Herrick. 2009. Google this!: using Google apps for collaboration and productivity. In Proceedings of the ACM SIGUCCS fall conference on User services conference (SIGUCCS '09). ACM, New York, NY, USA, 55-64. DOI=10.1145/1629501.1629513 http://doi.acm.org/10.1145/1629501.1629513

6) Rittinghouse,J.W., & Ransome,J.F. (2010). Cloud Computing Implementation, Management, and Security. New York: Taylor and Francis Group.

7) The Research and Application of Network Teaching Platform Based on Cloud Computing, Zhang Tao and Jiao Long, International Journal of Information and Education Technology, Vol. 1, No. 3, August 2011

8) Cloud Computing For Distributed University Campus: A Prototype Suggestion, http://www.pixelonline.net/edu_future/common/download/Paper_pdf/ENT30-Erkoc.pdf

9) L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, A break in the clouds: Towards a cloud definition, SIGCOMM Computer Communications Review,

10) N. Carr, The Big Switch: Rewiring the World, from Edison to Google.W. W. Norton & Co., New York, 2008.

11) M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, and R. Katz, Above the Clouds: A Berkeley View of Cloud Computing, UC Berkeley Reliable Adaptive Distributed Systems Laboratory White Paper, 2009.

12) N. Carr, The Big Switch: Rewiring the World, from Edison to Google.W. W. Norton & Co., New York, 2008.

13) Benson Vladlena, Morgan Stephanie. Student Experience and Ubiquitous Learning in Higher Education: Impact of Wireless and Cloud Applications // Creative Education. – Vol.4, No.8A. – 2013. – P.1-5. – [Electronic Resourse]. – Mode of access : http://www.scirp.org/journal/ce/ – Title from the screen.

14) Biswas Sourya. How Can Cloud Computing Help In Education? / Sourya Biswas. – [Electronic Resourse]. – Mode of access : http://www.cloudtweaks.com/2011/02/how-can-cloud-computing-help-ineducation/. – Title from the screen.

15) Britto Marwin. Cloud Computing in Higher Education / Marwin Britto // Library Student Journal. – [Electronic Resourse]. – Mode of access : http://www.librarystudentjournal.org/index.php/lsj/article/view/289/321. – Title from the screen.

16) CYPHER Learning [Electronic Resource] – Mode of access : URL : http://www.cypherlearning.com/. – Title from the screen. 6. Fundacion German Sanchez Ruiperez and IBM Implement a Cloud Computing Solution for Education [Electronic Resource] – Mode of access : URL : http://goliath.ecnext.com/coms2/gi_0199-13346074/Fundacion-German-SanchezRuiperez-and.html. – Title from the screen.

17) IBM Cloud Academy [Electronic Resource] – Mode of access : URL : http://www.ibm.com/solutions/education/cloudacademy/us/en. – Title from the screen.

18) Lepi K. The Future of Higher Educational and Cloud Computing [Electronic Resource] / Katie Lepi. – Mode of access : URL : http://www.edudemic.com/2013/02/higher-educational-and-cloud-computing. – Title from the screen.

19) Liu Jiayi. Cloud computing modernizes education in China [Electronic Resource] – Mode of access : URL : http://www.zdnet.com/cn/cloud-computing-modernizeseducation-in-china-7000015196/. – Title from the screen.

20) Семеріков С. О. Хмарні технології навчання: витоки / О. М. Маркова, С. О. Семеріков, А. М. Стрюк // Інформаційні технології і засоби навчання. – 2015. – №2 (46). – С. 29-44. – Режим доступу до журн. : http://journal.iitta.gov.ua/index.php/itlt/article/view/1234/916#.VfFO4NLtmko.

21) Санітарні норми мікроклімату виробничих приміщень ДСН 3.3.6.042-99. Постанова N 42 від 01.12.99. Режим доступу: www. URL: https://zakon.rada.gov.ua/rada/show/va042282-99

22) Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98. Затверджено Постановою Головного державного санітарного лікаря України 10 грудня 1998 р. N 7. Режим доступу: www. URL: https://zakon.rada.gov.ua/rada/show/v0007282-98

23) НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів». *Наказ від 09.01.98 №4.* Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/z0093-98

24) ГОСТ 12.1.044-89 «Система стандартов безопасности труда. Пожаровзрывоопасность веществ и материалов. Номенклатура показателей и методы их определения». Постанова від 12.12.1989 № 3683. Режим доступу: www. URL: http://online.budstandart.com/ru/catalog/doc-page?id_doc=51048

25) *ДСП 173-96 «Державні санітарні правила планування та забудови населених пунктів». Наказ від 19.06.1996 №173.* Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/z0379-96

26) TCO'07 Certified Displays. © 2007 Copyright TCO Development AB. Режим доступу: www. URL: https://tcocertified.com/files/2015/11/TCO-Certified-Displays-7.0.pdf

27) ДБН В.2.5-28:2018 «Природне і штучне освітлення». Режим доступу: www. URL: http://www.minregion.gov.ua/wp-content/uploads/ 2018/12/V2528-1.pdf

28) ДСТУ Б В.1.1-36:2016 «Визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою». Наказ від 15.06.2016 №158. Режим доступу: www. URL: https://zakon.rada.gov.ua/rada/show/v0158858-16

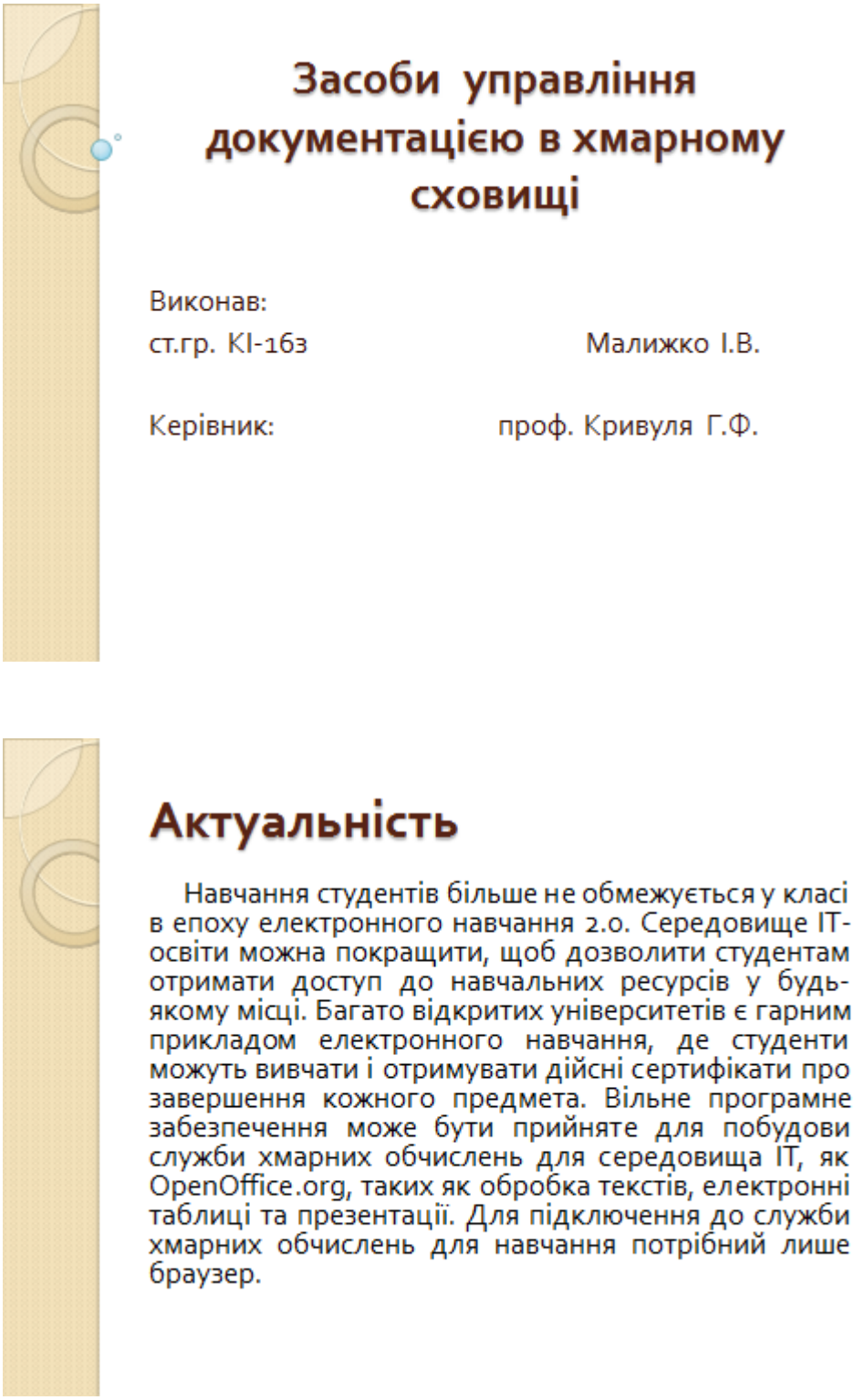
29) ГОСТ 12.1.004-91 «Система стандартов безопасности труда. Пожарная безопасность. Общие требования». Режим доступу: www. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=48679

30) НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні». Наказ від 30.12.2014 №1417. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/z0252-15

31) НАПБ Б.01.008-2018 «Про затвердження правил експлуатації та типових норм належності вогнегасників». Наказ від 15.01.2018 №25. Режим доступу: www. URL: http://search.ligazakon.ua/ l_doc2.nsf/link1/ RE31677.html

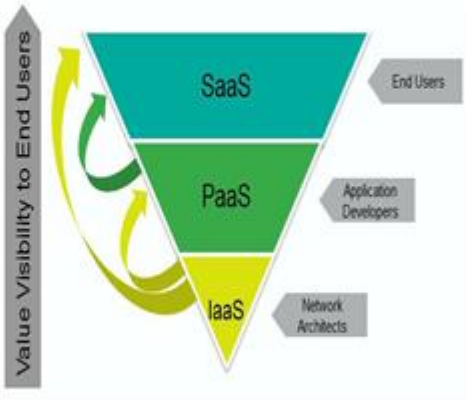
Додаток А

Комп’ютерна презентація



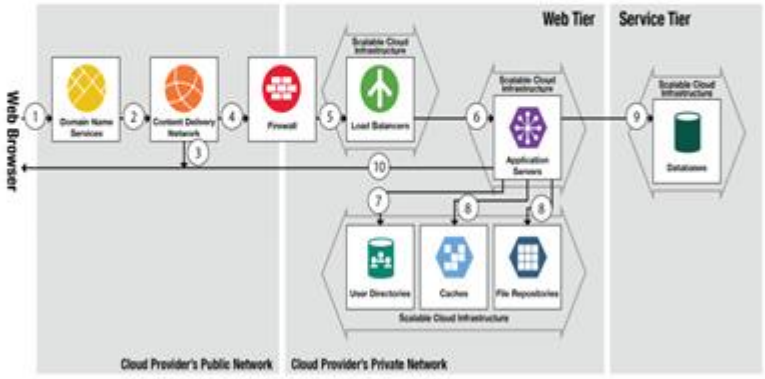
Хмарні обчислення

Архітектура хмарних обчислень

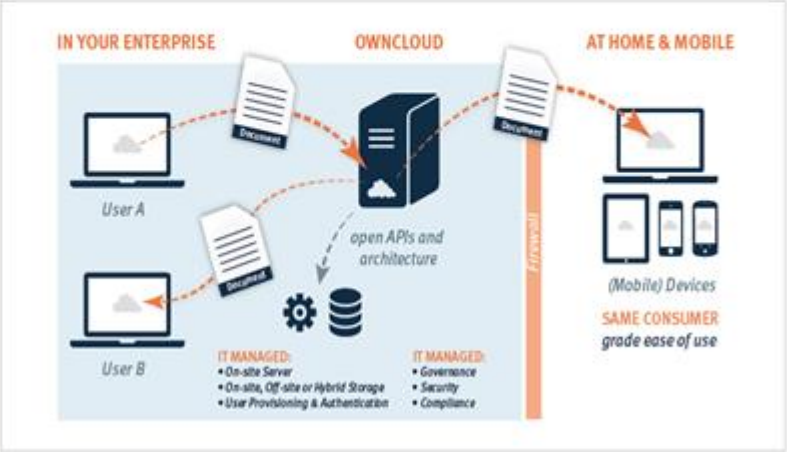


Хостинг веб-додатків Хмарної архітектури

Web Application Hosting Cloud Architecture



Можливості ownCloud з синхронізації даних



Конфігурація Apache

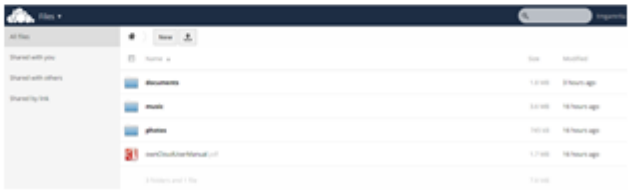
```
# cp /etc/webapps/owncloud/apache.example.conf /etc/httpd/conf/extra/owncloud.conf
```

```
Include conf/extra/owncloud.conf
```

```
LoadModule php5_module modules/libphp5.so
Include conf/extra/php5_module.conf
```

```
# chown -R http:http /usr/share/webapps/owncloud/
```

Доступ до веб-інтерфейсу ownCloud



Тестування інтерфейсу веб-сторінки для завантаження файлів

Висновки

Утримання десятків комп'ютерів в лабораторіях стає тягарем для системного адміністратора. Саме тому в дипломній роботі була запропонована бездискова кластерна обчислювальна середовище в комп'ютерному класі і розробка навчальної системи управління мережею. У цьому дипломі ми обговорюємо парадигму та характеристики «хмарних обчислень», моделі обслуговування та розгортання, реалізації хмарних сервісів у університетах, а також різні можливості та переваги Cloud Computing для університетів та академічних установ. Нарешті, ми пропонуємо прототип дизайну Cloud Computing для академічного середовища.