

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Мережева інфраструктура в хмарних середовищах на базі інтеграції AWS та Eucalyptus»

на здобуття освітнього ступеня магістра
зі спеціальності 122 Комп'ютерні науки
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні науки
(назва)

*Кваліфікаційна робота містить результати власних досліджень.
Використання ідей, результатів і текстів інших авторів мають посилання
на відповідне джерело*

(підпис)

Антон Сімонов
(Ім'я, ПРІЗВИЩЕ здобувача)

Виконав:
здобувач вищої освіти
група КНДМ-63

Антон Сімонов

Керівник:
науковий ступінь,
вчене звання

Микола Гніденко
д.т.н., професор, доцент

Рецензент:
науковий ступінь,
вчене звання

(Ім'я, ПРІЗВИЩЕ)

Київ 2024

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерних наук

Ступінь вищої освіти Магістр

Спеціальність Комп'ютерні науки

Освітньо-професійна програма Комп'ютерні науки

ЗАТВЕРДЖУЮ

Завідувач кафедру Комп'ютерних наук

_____ Віктор ВИШНІВСЬКИЙ
« _____ » _____ 2024 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

_____ Сімонову Антону Юрійовичу

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Мережева інфраструктура в хмарних середовищах на базі інтеграції AWS та Eucalyptus»

керівник кваліфікаційної роботи Микола Гніденко д.т.н., професор, доцент,
(Ім'я, ПРИЗВИЩЕ науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024р. №320

2. Строк подання кваліфікаційної роботи «15» грудня 2024р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, метод моделювання мережевої архітектури, експериментальне тестування інтеграційних рішень та їхню оцінку за технічними та економічними показниками.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

4.1. Дослідження методу моделювання мережевої архітектури.

4.2. Проектування мережевої інфраструктури та підбір технологій для її реалізації.

- 4.3. Розробка моделі інтегрованої мережевої інфраструктури та аналіз її ефективності.
5. Перелік графічного матеріалу: *презентація*
- 5.1 Основні методи візуалізації даних за допомогою діаграм та таблиць.
- 5.2 Підходи до проектування мережевої інфраструктури.
- 5.3 Приклади програмного коду.
- 5.4 Головні компоненти створеної інфраструктури.
6. Дата видачі завдання «16» вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	16.09-27.09.24	виконано
2	Аналіз методу моделювання мережевої інфраструктури та експериментального тестування інтеграційних рішень	30.09-11.10.24	виконано
3	Проектування та підбір технологій реалізації	14.10-25.10.24	виконано
4	Розробка мережевої інфраструктури	28.10-22.12.24	виконано
5	Головні компоненти створеної системи	25.11-29.11.24	виконано
6	Оформлення роботи: вступ, висновки, реферат	02.12-06.12.24	виконано
7	Розробка демонстраційних матеріалів	09.12-13.12.24	виконано

Здобувач вищої освіти

(підпис)

Антон Сімонов

(Ім'я, ПРІЗВИЩЕ)

Керівник

кваліфікаційної роботи

(підпис)

Микола Гніденко

(Ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 87 стор., 6 табл., 5 рис., 25 джерел.

Наукове завдання – розробка моделі інтегровано мережевої інфраструктури для проведення оцінки за технічними та економічними показниками використовуючи AWS та Eucalyptus.

Мета роботи – розробка методичних основ та практичних рекомендацій щодо створення ефективної мережевої інфраструктури в хмарних середовищах на базі інтеграції AWS та Eucalyptus.

Об'єкт дослідження – хмарні обчислювальні середовища, які функціонують на основі інтеграції публічних і приватних хмарних платформ.

Предмет дослідження є мережева інфраструктура хмарних обчислювальних середовищ із використанням інтеграції AWS та Eucalyptus.

Методи дослідження – аналітичний огляд літератури, моделювання мережевої архітектури, експериментальне тестування інтеграційних рішень та їхню оцінку за технічними та економічними показниками.

Короткий зміст роботи: Проведено аналіз методу моделювання хмарної архітектури. Розроблено модель інтегрованої мережевої архітектури. Було доведено, що гібридні хмарні середовища забезпечують унікальне поєднання масштабованості публічних хмар і контролю приватних платформ, що дозволяє вирішувати завдання сучасних організацій у динамічному бізнес-середовищі. Результатом дослідження підтвердження значного підвищення гнучкості управління ІТ-ресурсами за рахунок інтеграції AWS та Eucalyptus.

Ключові слова: хмарні сервіси, дослідження мережевої інфраструктури, метод моделювання мережевої архітектури, гібридні хмарні середовища.

ABSTRACT

Text part of the master's qualification work: 87 pages, 5 pictures, 6 table, 25 sources.

Scientific task is to develop an integrated network infrastructure model for conducting evaluations based on technical and economic indicators using AWS and Eucalyptus.

Goal of the work is to develop of methodological foundations and practical recommendations for creating an effective network infrastructure in cloud environments based on the integration of AWS and Eucalyptus.

Object of research – cloud computing environments that operate based on the integration of public and private cloud platforms.

Subject of research – the network infrastructure of cloud computing environments using the integration of AWS and Eucalyptus.

Research methods – an analytical literature review, network architecture modeling, experimental testing of integration solutions, and their evaluation based on technical and economic indicators.

Summary of the work: An analysis of the cloud architecture modeling method was conducted. An integrated network architecture model was developed. It was proven that hybrid cloud environments provide a unique combination of public cloud scalability and private platform control, enabling the resolution of modern organizations' challenges in a dynamic business environment. The study's results confirm a significant increase in IT resource management flexibility through the integration of AWS and Eucalyptus.

Keywords: cloud services, network infrastructure research, a network architecture modeling method, hybrid cloud environments.

ЗМІСТ

ВСТУП.....	9
1 ТЕОРЕТИЧНІ ОСНОВИ ХМАРНИХ ОБЧИСЛЕНЬ ТА МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ.....	10
1.1 Сутність та класифікація хмарних обчислень.....	10
1.2 Основи побудови мережевої інфраструктури в хмарних середовищах.....	18
1.3 Порівняння платформ AWS та Eucalyptus.....	22
2 ТЕХНОЛОГІЧНІ ОСНОВИ ІНТЕГРАЦІЇ AWS ТА EUCALYPTUS.....	27
2.1 Архітектура платформи AWS.....	27
2.2 Архітектура платформи Eucalyptus.....	31
2.3 Інструменти та методи інтеграції.....	38
3 РОЗРОБКА МОДЕЛІ ІНТЕГРОВАНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ.....	43
3.1 Постановка задачі проектування.....	43
3.2 Вибір програмного забезпечення та інструментів.....	47
3.3 Модель інтеграції AWS та Eucalyptus.....	52
4 АНАЛІЗ ЕФЕКТИВНОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІНТЕГРАЦІЇ ХМАРНИХ ПЛАТФОРМ.....	60
4.1 Показники ефективності інтеграції.....	60
4.2 Вплив інтеграції на продуктивність мережевої інфраструктури.....	69
4.3 Перспективи використання гібридних хмарних середовищ.....	73
Висновки.....	78
Перелік посилань.....	80
Додаток А.....	82

ВСТУП

Сучасний розвиток інформаційних технологій характеризується стрімким зростанням популярності хмарних обчислень. Це обумовлено потребою організацій і компаній в ефективному управлінні ресурсами, зменшенні витрат на IT-інфраструктуру, забезпеченні гнучкості та масштабованості своїх систем. Одними з ключових складових успішного функціонування хмарних середовищ є їхня мережева інфраструктура, що забезпечує інтеграцію, взаємодію та доступ до ресурсів. У зв'язку з цим важливим аспектом стає дослідження мережевої інфраструктури, яка базується на інтеграції популярних платформ, таких як Amazon Web Services (AWS) та Eucalyptus.

AWS є однією з найвідоміших і найрозвиненіших платформ хмарних обчислень, що забезпечує широкий спектр сервісів для зберігання даних, обробки інформації та розробки додатків. Водночас Eucalyptus пропонує унікальні можливості для створення приватних хмарних середовищ із високою сумісністю з AWS. Інтеграція цих двох платформ дозволяє організаціям оптимізувати процеси управління IT-інфраструктурою та забезпечити більш ефективне використання хмарних ресурсів. Дослідження у цій галузі є актуальними не лише з точки зору технічної реалізації, а й з позицій економічної ефективності, безпеки даних та екологічної стійкості IT-інфраструктури. У роботі зроблено спробу детально розглянути питання побудови мережевої інфраструктури в хмарних середовищах із використанням інтеграції AWS та Eucalyptus.

1 ТЕОРЕТИЧНІ ОСНОВИ ХМАРНИХ ОБЧИСЛЕНЬ ТА МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

1.1 Сутність та класифікація хмарних обчислень

Хмарні обчислення — це модель надання обчислювальних ресурсів, яка забезпечує доступ до інформаційних технологій через інтернет. Вони дозволяють користувачам зберігати, обробляти та передавати дані, використовуючи потужності віддалених серверів замість локальної IT-інфраструктури. Головною особливістю хмарних обчислень є те, що користувач отримує доступ до обчислювальних потужностей, програмного забезпечення чи зберігання даних у режимі реального часу, без необхідності купувати або обслуговувати власне обладнання [25].

Ключовими характеристиками хмарних обчислень, які відрізняють їх від традиційних моделей, є адаптивність, масштабованість і доступність. Адаптивність полягає в тому, що хмарні обчислення дозволяють швидко реагувати на зміну потреб користувача. Наприклад, якщо компанії раптово потрібні додаткові ресурси, такі як обчислювальна потужність або зберігання даних, вони можуть бути легко додані без необхідності оновлювати фізичне обладнання. Масштабованість хмарних обчислень означає здатність збільшувати або зменшувати обсяги ресурсів залежно від потреб, що особливо важливо для бізнесу зі змінним рівнем навантаження. У традиційних системах для розширення ресурсів часто необхідно проводити тривалі процедури з придбанням, налаштуванням і встановленням нового обладнання. Хмари, навпаки, забезпечують це автоматично, знижуючи витрати часу та коштів.

Доступність є ще однією важливою особливістю. Хмарні обчислення доступні з будь-якого місця, де є підключення до інтернету. Це дозволяє користувачам працювати з даними та додатками незалежно від їхнього фізичного місцезнаходження, сприяючи мобільності та зручності. До того ж провайдери хмарних послуг забезпечують високу надійність, адже обчислення здійснюються

на кількох серверах, що зменшує ризики втрати даних через вихід з ладу одного з них.

Окрім цього, хмарні обчислення відзначаються високим рівнем автоматизації, що дозволяє користувачам отримувати ресурси "на вимогу" без ручного втручання адміністраторів. Усе це робить хмарні обчислення революційним підходом до управління обчислювальними потужностями та ресурсами, який змінює спосіб, у який працюють організації, забезпечуючи їм конкурентні переваги в сучасному світі. Ще однією важливою особливістю хмарних обчислень є економічна ефективність. Використання хмарної інфраструктури дозволяє значно скоротити витрати на придбання, обслуговування та оновлення локального обладнання. Замість того, щоб інвестувати у створення власного дата-центру, компанії можуть оплачувати лише ті ресурси, які вони фактично використовують, за моделлю "pay-as-you-go". Це особливо вигідно для малого та середнього бізнесу, який часто не має можливості підтримувати масштабну ІТ-інфраструктуру [23].

Безпека та резервування даних також є вагомими перевагами хмарних обчислень. Провайдери хмарних послуг зазвичай пропонують високі стандарти кібербезпеки, використовуючи шифрування, багаторівневу аутентифікацію та інші засоби захисту даних. Крім того, дані, що зберігаються в хмарі, автоматично резервуються, що мінімізує ризик їхньої втрати через апаратні збої або людський фактор.

Хмарні обчислення також сприяють інноваціям. Завдяки їхній гнучкості компанії можуть швидко тестувати нові ідеї, розгортати додатки та впроваджувати технології, які раніше були недоступні через високі початкові витрати або технічні обмеження. Наприклад, платформи хмарних обчислень надають інструменти для роботи з великими даними (Big Data), штучним інтелектом (AI) та машинним навчанням (ML), що відкриває нові горизонти для досліджень та бізнес-рішень. Крім того, хмарні обчислення активно підтримують екологічну стійкість. За рахунок оптимізації використання ресурсів вони дозволяють значно зменшити викиди вуглецю, порівняно з традиційними дата-центрами, які часто працюють із

надлишковими потужностями. Центральне управління великими обчислювальними ресурсами в хмарі дає змогу ефективно розподіляти навантаження між серверами, що зменшує їхнє енергоспоживання.

Отже, хмарні обчислення представляють собою інноваційний підхід до організації IT-інфраструктури, який забезпечує адаптивність, масштабованість, доступність, економічність і безпеку. Вони трансформують підходи до роботи з даними, відкриваючи нові можливості для бізнесу, науки та повсякденного життя. У той же час, їхній розвиток супроводжується викликами, такими як забезпечення конфіденційності даних, дотримання законодавчих норм у різних юрисдикціях та необхідність адаптації організацій до нових технологічних процесів. У цьому контексті дослідження сутності та характеристик хмарних обчислень, а також пошук шляхів подолання можливих обмежень є актуальним і стратегічно важливим завданням сучасної IT-індустрії [24]. У таблиці 1.1 продемонстровано основні моделі обслуговування в хмарних сервісах.

Таблиця 1.1. Основні моделі обслуговування в хмарних обчисленнях

Модель обслуговування	Опис	Приклади використання
IaaS (Infrastructure as a Service)	Забезпечує базову інфраструктуру, таку як віртуальні сервери, мережі та сховища даних. Користувачі отримують контроль над операційними системами, але відповідальність за управління інфраструктурою лежить на провайдері.	Створення віртуальних машин, розгортання серверів, зберігання великих обсягів даних.

Продовження таблиці 1.1. Основні моделі обслуговування в хмарних обчисленнях

PaaS (Platform as a Service)	Забезпечує середовище для розробки, тестування та розгортання додатків. Користувачі отримують готові платформи, що спрощують процес створення додатків, без необхідності управління інфраструктурою.	Розробка веб-додатків, управління базами даних, автоматизація CI/CD процесів.
SaaS (Software as a Service)	Надає доступ до готових програмних рішень через інтернет. Користувачі користуються додатками без необхідності їхнього встановлення та обслуговування.	Користування корпоративними програмами, такими як Office 365, Google Workspace, CRM-системи.

Моделі розгортання хмарних обчислень визначають, як організовано інфраструктуру, які ресурси надаються користувачам і хто відповідає за їх управління. Залежно від потреб організацій, бюджету, вимог до безпеки та доступності, обирають різні типи моделей розгортання. Основними серед них є публічні, приватні, гібридні та мультихмарні середовища [22].

Публічні хмарні середовища є найпоширенішою моделлю розгортання. У цій моделі ресурси, такі як сервери, сховища даних і програми, надаються провайдером хмарних послуг (наприклад, AWS, Google Cloud, Microsoft Azure) і доступні через інтернет. Публічні хмари ідеально підходять для організацій, які потребують гнучкості та масштабованості, але не мають бажання або можливості інвестувати у власну інфраструктуру. Однією з ключових переваг публічних хмар є те, що користувачі оплачують лише ті ресурси, які вони використовують. Водночас

недоліком може бути менший контроль над безпекою даних, оскільки інфраструктура розташована поза межами організації [20].

Приватні хмарні середовища створюються для використання лише однією організацією. Інфраструктура може бути розташована у власному дата-центрі компанії або орендована у провайдера послуг, але в будь-якому випадку доступ до ресурсів обмежений лише для обраних користувачів. Така модель забезпечує високий рівень безпеки, конфіденційності даних та повний контроль над інфраструктурою. Приватні хмари найчастіше використовуються організаціями, які працюють у секторах із суворими регуляторними вимогами, наприклад, у фінансовій сфері чи охороні здоров'я. Проте значним недоліком приватних хмар є високі витрати на їх створення та обслуговування.

Гібридні хмарні середовища об'єднують переваги публічних і приватних хмар, дозволяючи організаціям використовувати обидві моделі залежно від потреб. Наприклад, компанія може зберігати чутливі дані у приватній хмарі, а для менш критичних завдань, таких як розробка або тестування додатків, використовувати публічну хмару. Цей підхід забезпечує більшу гнучкість і дозволяє ефективно розподіляти навантаження між системами. Гібридні хмари часто використовуються великими корпораціями, які прагнуть зберегти контроль над критичними даними, але водночас мають потребу у масштабованості.

Мультихмарні середовища є більш складною моделлю, яка передбачає використання кількох публічних і приватних хмар одночасно. Організації обирають цю модель, щоб уникнути залежності від одного провайдера послуг, що забезпечує підвищену надійність і безперервність бізнес-процесів. Наприклад, компанія може використовувати одну хмару для аналітики великих даних, а іншу для зберігання даних. Мультихмарні середовища також дозволяють оптимізувати витрати, оскільки організація може вибирати найбільш вигідні сервіси кожного з провайдерів.

Вибір моделі розгортання хмарних обчислень залежить від багатьох факторів, таких як рівень конфіденційності даних, обсяг бюджету, потреба в масштабованості та специфіка галузі. Кожна з моделей має свої переваги та

обмеження, і їх грамотне використання дозволяє організаціям ефективно вирішувати завдання та досягати стратегічних цілей. Хмарні обчислення пропонують широкий спектр сервісів і моделей обслуговування, які дозволяють організаціям ефективно впроваджувати, розробляти та підтримувати ІТ-рішення. Основними моделями обслуговування є IaaS (інфраструктура як послуга), PaaS (платформа як послуга) та SaaS (програмне забезпечення як послуга). Кожна з цих моделей виконує певну роль у хмарних обчисленнях і задовольняє різні потреби користувачів [21].

IaaS (Infrastructure as a Service) забезпечує користувачів базовою інфраструктурою, включаючи віртуальні сервери, мережі, сховища даних і операційні системи. Ця модель дає можливість організаціям орендувати необхідні ресурси замість придбання власного обладнання, що знижує початкові витрати та витрати на обслуговування. IaaS дозволяє компаніям гнучко реагувати на зміну вимог бізнесу, масштабуючи ресурси відповідно до поточного навантаження. Це особливо важливо для великих проєктів, таких як обробка великих обсягів даних чи розробка складних ІТ-рішень. Водночас користувачі IaaS залишаються відповідальними за управління операційними системами, додатками та безпекою.

PaaS (Platform as a Service) забезпечує готове середовище для розробки, тестування та розгортання додатків. У цій моделі хмарні провайдери пропонують платформу, яка включає інструменти для програмування, бази даних, сервери додатків і середовища виконання коду. Це спрощує процес розробки, оскільки програмісти можуть зосередитися виключно на написанні коду, не турбуючись про інфраструктуру чи сумісність компонентів. PaaS є ідеальним рішенням для компаній, які займаються розробкою програмного забезпечення, адже ця модель знижує витрати часу на підготовку середовища та автоматизує багато рутинних завдань, таких як оновлення бібліотек або налаштування серверів.

SaaS (Software as a Service) є моделлю, у якій користувачі отримують доступ до готового програмного забезпечення через інтернет. Вона дозволяє організаціям використовувати програми без необхідності їх встановлення та обслуговування на локальних пристроях. Це охоплює широкий спектр рішень, від офісних додатків до

спеціалізованих корпоративних систем, таких як CRM, ERP або системи управління контентом. SaaS знижує технічні бар'єри для користувачів, оскільки вони отримують готовий продукт, що регулярно оновлюється та підтримується провайдером. Для компаній це означає можливість швидкого впровадження сучасних технологій без значних інвестицій у локальну IT-інфраструктуру [1].

Кожна з цих моделей впливає на розробку та використання IT-рішень у різний спосіб. IaaS дозволяє організаціям створювати гнучкі, масштабовані системи, орієнтовані на високі навантаження, при цьому зберігаючи контроль над усіма аспектами інфраструктури. PaaS прискорює процес розробки програмного забезпечення, знижуючи складність управління технічними компонентами. SaaS, у свою чергу, демократизує доступ до сучасних технологій, надаючи малим і середнім компаніям можливість використовувати ті ж інструменти, що й великі корпорації [2].

Важливо зазначити, що ці моделі можуть поєднуватися в межах однієї організації для досягнення найкращих результатів. Наприклад, компанія може використовувати IaaS для створення власного дата-центру, PaaS для розробки специфічних додатків і SaaS для управління внутрішніми процесами. Таким чином, хмарні обчислення не тільки оптимізують управління IT-ресурсами, але й сприяють розвитку інновацій, розширюючи горизонти можливостей для бізнесу. Використання хмарних обчислень приносить численні переваги, які змінюють підходи до управління IT-інфраструктурою, розширюють можливості організацій та сприяють їхньому розвитку. Однак із цими перевагами пов'язані і певні ризики, які потребують уваги. Оцінка впливу хмарних обчислень на безпеку даних, економічну ефективність та екологічність IT-інфраструктур дає змогу зрозуміти їхню доцільність у сучасному світі [3].

Однією з головних переваг хмарних обчислень є їхня економічна ефективність. Організації можуть знизити витрати на створення та обслуговування локальної інфраструктури, орендуючи необхідні ресурси у хмарних провайдерів. Це особливо вигідно для малого та середнього бізнесу, який часто не має доступу до значних капітальних інвестицій. Крім того, модель оплати "pay-as-you-go"

дозволяє оплачувати лише ті ресурси, які фактично використовуються, що оптимізує витрати та підвищує фінансову гнучкість. Однак із цим пов'язаний ризик прихованих витрат, коли організації не завжди правильно оцінюють обсяги використання ресурсів або стикаються з додатковими витратами на передачу даних між хмарами.

Хмарні обчислення також позитивно впливають на екологічність ІТ-інфраструктури. Завдяки централізованому управлінню ресурсами хмарні провайдери можуть досягти високої енергоефективності. Великі дата-центри, що використовуються для підтримки хмарних сервісів, зазвичай оснащені сучасними системами охолодження та енергозбереження. Це дозволяє зменшити викиди вуглекислого газу в порівнянні з численними малоефективними локальними серверними установками. Водночас, зростання популярності хмарних обчислень призводить до збільшення загального енергоспоживання, і це може викликати екологічні виклики, якщо джерела енергії для дата-центрів не є відновлюваними.

Щодо безпеки даних, хмарні обчислення пропонують високий рівень захисту завдяки багатшаровим системам безпеки, таким як шифрування, контроль доступу та регулярний моніторинг загроз. Багато хмарних провайдерів дотримуються суворих стандартів безпеки, що забезпечує захист даних від несанкціонованого доступу. Однак одним із головних ризиків є втрата контролю над даними, оскільки вони зберігаються на сторонніх серверах. Це викликає занепокоєння, особливо для організацій із чутливою інформацією, такою як фінансові установи чи медичні заклади. Також залишається ризик кібератак, які можуть призвести до витоку інформації, а відновлення доступу до даних після збоїв у хмарі іноді залежить від швидкості реакції провайдера.

Іншою перевагою хмарних обчислень є їхня масштабованість і гнучкість. Організації можуть швидко адаптувати свої ресурси до змін у попиті, наприклад, збільшити обчислювальні потужності під час пікових навантажень або зменшити їх після завершення проєкту. Це підвищує операційну ефективність та дозволяє бізнесу зосередитися на стратегічних цілях. Однак із цим також пов'язані технічні

ризиків, такі як затримки в роботі або залежність від стабільності інтернет-з'єднання [4].

Таким чином, хмарні обчислення мають значний потенціал для трансформації ІТ-інфраструктури завдяки своїм перевагам у гнучкості, економічності та екологічності. Водночас їх використання вимагає ретельного аналізу ризиків, пов'язаних із безпекою даних, прихованими витратами та технічними викликами. Збалансований підхід до впровадження хмарних обчислень дозволяє організаціям максимально ефективно використовувати їхній потенціал, зберігаючи при цьому високий рівень захисту та надійності.

1.2 Основи побудови мережевої інфраструктури в хмарних середовищах

Побудова мережевої інфраструктури в хмарних середовищах є ключовим аспектом, який забезпечує функціональність, надійність і масштабованість хмарних послуг. Це складний процес, що включає розробку архітектури, налаштування мережевих з'єднань, управління трафіком і забезпечення безпеки. Основою побудови такої інфраструктури є інтеграція апаратного та програмного забезпечення для створення оптимального середовища, яке відповідає вимогам конкретного хмарного рішення. Важливим етапом побудови мережевої інфраструктури є визначення архітектури хмарного середовища. Це включає вибір моделі розгортання (публічна, приватна, гібридна або мультихмарна), яка відповідатиме потребам організації. Архітектура має враховувати такі аспекти, як обсяг трафіку, рівень доступності, розподіл даних між регіонами та вимоги до безпеки. Основним завданням є забезпечення стабільного та швидкого з'єднання між користувачами, серверами і додатками, що працюють у хмарі [5].

Одним із центральних елементів мережевої інфраструктури є віртуальні приватні мережі (VPN), які забезпечують безпечний зв'язок між локальною інфраструктурою організації та хмарними ресурсами. VPN дозволяють створювати тунелі для передачі даних через загальнодоступні мережі, що мінімізує ризик перехоплення інформації. Віртуальні мережі також допомагають сегментувати трафік і забезпечувати оптимальне управління ресурсами.

Крім VPN, у хмарних середовищах активно використовуються віртуальні мережеві функції (VNF), які дозволяють автоматизувати процеси налаштування мережі. Це забезпечує швидку адаптацію інфраструктури до змінних умов і сприяє більш ефективному використанню ресурсів. Завдяки програмно-визначеним мережам (SDN), організації можуть централізовано управляти маршрутизацією трафіку, налаштуванням політик безпеки та оптимізацією роботи мережі.

Безпека є ще одним критично важливим аспектом при побудові мережевої інфраструктури в хмарних середовищах. Для захисту даних використовуються шифрування, системи виявлення загроз, брандмауери та багатофакторна аутентифікація. Важливим завданням є забезпечення відповідності нормативним вимогам, зокрема щодо конфіденційності та обробки персональних даних. Рішення, які використовуються в хмарній інфраструктурі, мають забезпечувати високу надійність і мінімізувати ризик несанкціонованого доступу.

Ще одним важливим елементом є балансування навантаження. У хмарних середовищах це досягається за допомогою спеціальних механізмів, які рівномірно розподіляють трафік між серверами, щоб уникнути перевантаження окремих вузлів і забезпечити високу продуктивність додатків. Це особливо важливо для масштабованих систем, які обслуговують велику кількість користувачів. Інтеграція з іншими хмарними платформами також є важливим аспектом побудови мережевої інфраструктури. У сучасних умовах багато організацій використовують мультихмарні середовища, що вимагає забезпечення сумісності між різними платформами, такими як AWS, Google Cloud і Microsoft Azure. Це досягається через використання стандартних протоколів і API, які спрощують обмін даними та управління ресурсами.

Отже, побудова мережевої інфраструктури в хмарних середовищах є багатогранним процесом, який охоплює широкий спектр технологій та підходів. Основною метою є створення ефективного, безпечного і масштабованого середовища, яке відповідає потребам користувачів і забезпечує високу продуктивність хмарних рішень. Успіх у цій сфері залежить від грамотного планування, впровадження передових технологій і постійного моніторингу роботи

інфраструктури. Після побудови базової мережевої інфраструктури важливим етапом є її оптимізація та моніторинг для забезпечення стабільності та ефективності роботи. Хмарні середовища працюють у динамічних умовах, де кількість користувачів, обсяги трафіку та вимоги до ресурсів постійно змінюються. Для цього необхідно використовувати спеціалізовані інструменти для моніторингу, які дозволяють відстежувати стан мережі в режимі реального часу, аналізувати трафік і оперативно виявляти потенційні проблеми.

Моніторинг забезпечує можливість аналізу продуктивності системи, виявлення "вузьких місць" у мережі та прогнозування навантаження. Наприклад, інструменти аналізу трафіку можуть показати, які сервіси використовуються найбільше, що дозволяє налаштувати балансування навантаження або додати ресурси в потрібних вузлах. Також важливим є моніторинг безпеки, який включає відстеження підозрілих активностей, спроб несанкціонованого доступу чи атак типу DDoS. Це дає змогу швидко реагувати на загрози, захищаючи дані та забезпечуючи безперервність роботи систем.

Іншим аспектом оптимізації є автоматизація управління мережею. Завдяки використанню програмно-визначених мереж (SDN) та хмарних оркестраторів можна зменшити час, необхідний для виконання рутинних завдань, таких як налаштування нових серверів або зміна маршрутів трафіку. Автоматизація також сприяє кращій адаптивності мережевої інфраструктури до змін у вимогах бізнесу або технологічних умовах.

Щодо забезпечення доступності, особливу увагу потрібно приділити побудові резервних механізмів. У хмарних середовищах використовуються принципи надлишковості та географічного розподілу даних для підвищення стійкості систем. Наприклад, дані можуть зберігатися одночасно в кількох дата-центрах, розташованих у різних регіонах, що забезпечує доступність навіть у випадку збою в одному з них. Це особливо важливо для критично важливих додатків, які повинні працювати безперебійно.

Ще одним напрямом розвитку мережевої інфраструктури є інтеграція із сучасними технологіями, такими як штучний інтелект і машинне навчання. Ці

технології використовуються для автоматизованого аналізу трафіку, прогнозування навантаження та оптимізації ресурсів. Наприклад, алгоритми машинного навчання можуть визначати пікові періоди активності користувачів і автоматично масштабувати ресурси для забезпечення стабільної роботи додатків. Такі підходи дозволяють не лише підвищити продуктивність мережі, а й зменшити витрати за рахунок більш раціонального використання ресурсів. Перспективи розвитку мережевої інфраструктури в хмарних середовищах також пов'язані із впровадженням нових стандартів, таких як 5G, що забезпечують швидший і більш стабільний доступ до хмарних ресурсів. Збільшення пропускної здатності та зниження затримок відкривають нові можливості для реалізації інноваційних рішень, таких як Інтернет речей (IoT), розподілені обчислення та автоматизовані системи управління. На рисунку 1.1 показана базова архітектура побудови мережевої інфраструктури.

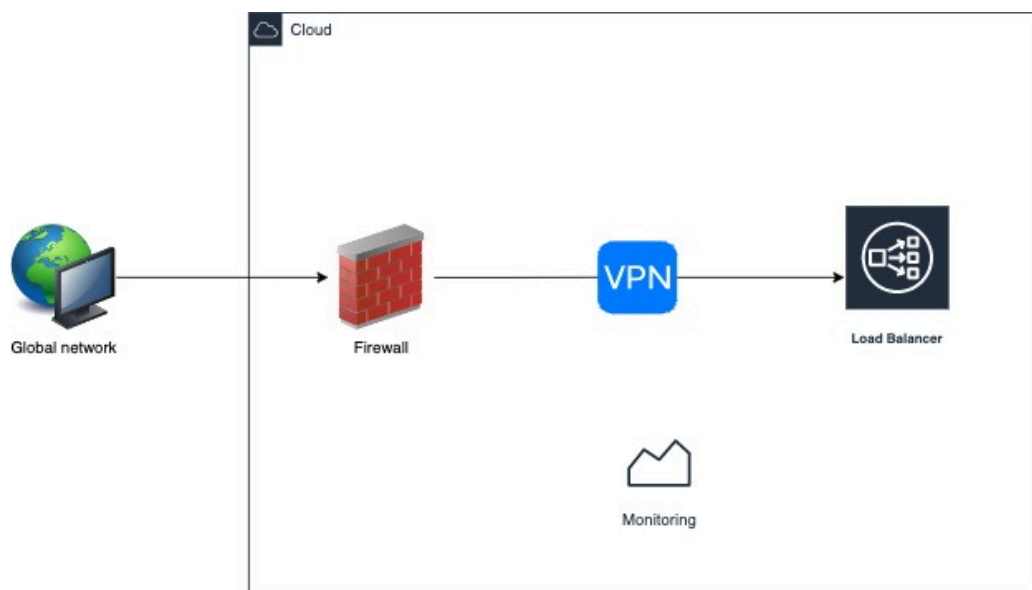


Рисунок 1.1 – Діаграма побудови мережевої інфраструктури

У підсумку, мережева інфраструктура в хмарних середовищах є не просто технічним рішенням, а основою для створення цифрових екосистем, які підтримують сучасний бізнес, науку та повсякденне життя. Її побудова та розвиток вимагають постійного вдосконалення, впровадження нових технологій і врахування змінних потреб користувачів. Ефективно спроектована та добре

оптимізована мережа є запорукою успішної роботи хмарних сервісів і платформа для майбутніх інновацій.

1.3 Порівняння платформ AWS та Eucalyptus

Amazon Web Services (AWS) і Eucalyptus є популярними платформами для хмарних обчислень, проте вони мають суттєві відмінності в концепціях, можливостях і сферах застосування. AWS є провідною комерційною платформою, яка пропонує широкий спектр хмарних послуг у публічному середовищі, тоді як Eucalyptus зосереджується на створенні приватних хмар, забезпечуючи сумісність з інфраструктурою AWS. Це робить їх доповнюваними в певних сценаріях, але також підкреслює різницю у фокусі і підходах.

AWS відома своєю масштабістю та різноманітністю сервісів. Вона пропонує інфраструктурні (IaaS), платформні (PaaS) та програмні (SaaS) рішення, які включають віртуальні машини, зберігання даних, бази даних, аналітику, машинне навчання та інші інструменти. Її перевага полягає у можливості працювати з глобально розподіленими дата-центрами, що забезпечує низькі затримки та високу доступність для користувачів у всьому світі. AWS також пропонує розширені функції для управління трафіком, балансування навантаження та масштабування ресурсів, що робить її ідеальним вибором для великих корпоративних систем і стартапів, які потребують глобальної присутності [6].

Eucalyptus, з іншого боку, зосереджується на побудові приватних хмар і забезпеченні сумісності з API AWS. Це дозволяє організаціям, які вже використовують AWS, інтегрувати приватні хмари на базі Eucalyptus у свої існуючі системи. Однією з ключових переваг Eucalyptus є можливість зберігати дані та обчислювальні ресурси в межах локальної інфраструктури організації, що забезпечує вищий рівень контролю та конфіденційності. Ця платформа ідеально підходить для компаній, які працюють у секторах з суворими регуляторними вимогами, наприклад, у фінансовій сфері чи охороні здоров'я. Щодо масштабованості, AWS пропонує необмежені можливості завдяки своїм глобальним ресурсам, тоді як Eucalyptus обмежена локальною інфраструктурою

організації. Це означає, що для Eucalyptus масштабування залежить від можливостей апаратного забезпечення, яке є у розпорядженні організації. AWS також забезпечує гнучкі моделі оплати, що дозволяє користувачам оплачувати лише фактично використані ресурси. Натомість Eucalyptus вимагає початкових інвестицій у створення локальної інфраструктури, але надалі забезпечує стабільні витрати.

У питаннях безпеки обидві платформи мають свої переваги. AWS пропонує розширені інструменти для захисту даних, такі як шифрування, багатофакторна аутентифікація та системи виявлення загроз. Однак дані в AWS зберігаються на серверах, які фізично розташовані у власності провайдера, що може викликати занепокоєння в організацій, які мають особливі вимоги до конфіденційності. Eucalyptus дозволяє зберігати всі дані локально, що мінімізує ризик несанкціонованого доступу, але безпека залежить від внутрішніх ресурсів та компетенції команди організації. Інтеграція з іншими сервісами є ще однією важливою відмінністю. AWS надає широкий вибір інструментів для інтеграції, включаючи сервіси для роботи з великими даними, штучним інтелектом та Інтернетом речей (IoT). Це робить AWS привабливим для інноваційних проєктів. Eucalyptus, у свою чергу, забезпечує базову функціональність для управління хмарними ресурсами, але її можливості в галузі інтеграції обмежені в порівнянні з AWS.

AWS і Eucalyptus представляють різні підходи до хмарних обчислень, орієнтуючись на різні аудиторії та потреби. AWS пропонує масштабованість, глобальну доступність і широкий набір інструментів, що робить її лідером серед публічних хмарних платформ. Eucalyptus, навпаки, фокусується на приватних хмарах і забезпеченні сумісності з AWS, що дозволяє організаціям зберігати контроль над своїми даними, залишаючись гнучкими. Вибір між цими платформами залежить від конкретних завдань і вимог організації. Важливою складовою порівняння платформ AWS та Eucalyptus є їхнє практичне застосування у реальних сценаріях. AWS завдяки своїй масштабованості та глобальній інфраструктурі ідеально підходить для компаній, які працюють на міжнародних

ринках, стартапів, які швидко зростають, і організацій, що потребують динамічного масштабування обчислювальних ресурсів. Наприклад, AWS часто використовується для розгортання великих веб-додатків, обробки великих обсягів даних або впровадження машинного навчання завдяки своїм спеціалізованим сервісам, таким як Amazon S3, EC2 та SageMaker.

Eucalyptus, у свою чергу, більше орієнтований на внутрішні потреби організацій, які прагнуть забезпечити повний контроль над своїми обчислювальними ресурсами. Наприклад, у медичних або фінансових установах, де вимоги до конфіденційності даних є критичними, Eucalyptus дозволяє створювати приватні хмарні середовища, які забезпечують інтеграцію із внутрішніми системами організації. Це особливо актуально для компаній, які працюють у юрисдикціях із суворими регуляторними нормами, такими як GDPR в Європі.

Ще одним аспектом, який слід враховувати, є вартість. AWS, як правило, вимагає менших початкових інвестицій, оскільки користувачі оплачують лише ті ресурси, які вони використовують. Це робить платформу привабливою для стартапів та малих компаній, які не мають значних фінансових ресурсів на створення власної інфраструктури. Однак у довгостроковій перспективі вартість користування AWS може зрости, особливо якщо організація інтенсивно використовує ресурси хмари. Eucalyptus вимагає більших початкових вкладень у створення приватної інфраструктури, але забезпечує стабільні та передбачувані витрати на її обслуговування. Обидві платформи також можуть використовуватися разом у гібридних хмарних середовищах, де AWS забезпечує масштабованість і гнучкість для певних завдань, а Eucalyptus використовується для обробки та зберігання конфіденційних даних у межах організації. Це дозволяє отримати переваги обох платформ і одночасно мінімізувати їхні недоліки.

Перспективи розвитку цих платформ також заслуговують уваги. AWS продовжує розширювати свій асортимент сервісів і вдосконалювати інструменти для роботи з великими даними, штучним інтелектом і хмарними обчисленнями. Інновації, які впроваджує AWS, підтримують її лідерську позицію на ринку

публічних хмар. Eucalyptus, хоч і має менший масштаб, також продовжує адаптуватися до сучасних викликів, забезпечуючи сумісність із новими API AWS та інтеграцію із сучасними корпоративними системами. В таблиці 1.2 відображене порівняння двох платформ.

Таблиця 1.2 Порівняння платформ AWS та Eucalyptus

Характеристика	AWS	Eucalyptus
Модель розгортання	Публічна хмара	Приватна хмара
Сфери застосування	Глобальні веб-додатки, Big Data, AI	Організації з високими вимогами до конфіденційності
Масштабованість	Необмежена	Обмежена інфраструктурою організації
Контроль над даними	Обмежений (дані зберігаються на серверах провайдера)	Повний контроль (дані зберігаються локально)
Інтеграція з іншими сервісами	Широка інтеграція з інструментами AI, ML, IoT	Обмежена інтеграція з іншими сервісами, але сумісність з AWS API
Початкові витрати	Мінімальні (оплата за використання ресурсів)	Високі (необхідність створення власної інфраструктури)
Довгострокова вартість	Висока залежно від інтенсивності використання	Стабільна та передбачувана
Безпека	Розширені інструменти безпеки, але ризик витоку даних у публічній хмарі	Високий рівень безпеки завдяки локальному зберіганню даних
Тип організацій	Стартапи, міжнародні корпорації, проекти з високим трафіком	Медичні, фінансові установи, урядові організації

Отже, вибір між AWS і Eucalyptus залежить від конкретних завдань, які стоять перед організацією. AWS підходить для завдань, що потребують глобального масштабу та гнучкості, тоді як Eucalyptus краще адаптований для локальних потреб та забезпечення конфіденційності. У багатьох випадках найбільш оптимальним рішенням є комбінований підхід, який дозволяє використовувати сильні сторони обох платформ для досягнення стратегічних цілей.

2 ТЕХНОЛОГІЧНІ ОСНОВИ ІНТЕГРАЦІЇ AWS ТА EUCALYPTUS

2.1 Архітектура платформи AWS

Архітектура платформи Amazon Web Services (AWS) є складною багатошаровою системою, яка забезпечує надання хмарних послуг у глобальному масштабі. Вона побудована з урахуванням масштабованості, доступності, безпеки та економічної ефективності, що дозволяє користувачам реалізовувати різноманітні обчислювальні сценарії. Архітектура AWS складається з кількох основних компонентів і рівнів, які працюють разом для забезпечення безперервної роботи хмарної інфраструктури. AWS використовує глобальну інфраструктуру, яка складається з регіонів та зон доступності. Регіони представляють собою географічно розташовані області, де AWS розгортає свої ресурси. Кожен регіон має кілька зон доступності, які є ізольованими дата-центрами. Це забезпечує високу доступність і стійкість до збоїв. Якщо одна зона доступності виходить з ладу, ресурси автоматично перемикаються на іншу зону, що мінімізує ризик переривання роботи [7].

Основою архітектури AWS є віртуальні приватні хмари (VPC), які дозволяють створювати ізольовані мережеві середовища для користувачів. VPC надають інструменти для налаштування маршрутизації, підмереж, брандмауерів і шлюзів. Це дозволяє користувачам контролювати доступ до своїх ресурсів та інтегрувати їх з локальними мережами через VPN або прямі підключення.

AWS також включає рівень обчислень, який забезпечується через Amazon EC2 (Elastic Compute Cloud). EC2 дозволяє користувачам запускати віртуальні сервери з різними конфігураціями залежно від потреб. Сервери можуть масштабуватися автоматично, реагуючи на зміну навантаження, що забезпечує гнучкість і економічну ефективність. Інші сервіси, такі як AWS Lambda, дозволяють виконувати обчислення без необхідності управління серверами, що спрощує розробку додатків [8].

Система зберігання даних є ще одним ключовим компонентом архітектури AWS. Amazon S3 (Simple Storage Service) забезпечує масштабоване сховище для

файлів і об'єктів, яке підтримує високу доступність і стійкість до збоїв. Для структурованих даних використовується Amazon RDS (Relational Database Service), який підтримує популярні системи управління базами даних, такі як MySQL, PostgreSQL та Oracle. Крім того, AWS пропонує сервіси для роботи з великими обсягами даних, такі як Amazon Redshift для аналітики та Amazon DynamoDB для обробки неструктурованих даних.

Мережевий рівень архітектури AWS забезпечує швидкий і безпечний доступ до ресурсів через сервіси, такі як Amazon Route 53 для управління доменними іменами, Amazon CloudFront для доставки контенту та Elastic Load Balancing для балансування навантаження. Ці інструменти забезпечують оптимальну продуктивність додатків і стабільність роботи навіть при високих навантаженнях [9].

Безпека є фундаментальним елементом архітектури AWS. Платформа пропонує багатошаровий захист, включаючи шифрування даних, багатофакторну аутентифікацію, контроль доступу на основі ролей і автоматизовані системи виявлення загроз. AWS також відповідає міжнародним стандартам безпеки, таким як GDPR, HIPAA та ISO 27001, що робить її привабливою для організацій із суворими вимогами до конфіденційності даних. Крім основних рівнів, архітектура AWS включає численні сервіси для роботи з великими даними, штучним інтелектом, машинним навчанням та Інтернетом речей (IoT). Наприклад, Amazon SageMaker дозволяє розробляти, навчати та розгортати моделі машинного навчання, а AWS IoT забезпечує обробку даних від підключених пристроїв.

Узагальнюючи, архітектура AWS є універсальною та масштабованою, що дозволяє вирішувати широкий спектр завдань — від розгортання веб-додатків до аналізу великих даних і розробки інноваційних рішень на основі штучного інтелекту. На рисунку 2.1 зображена базова архітектура AWS. Її гнучкість, безпека та глобальна доступність роблять AWS однією з провідних хмарних платформ у світі. Одним із ключових аспектів архітектури AWS є автоматизація процесів управління інфраструктурою. AWS надає інструменти, які дозволяють автоматизувати розгортання, моніторинг, оновлення та управління ресурсами.

Наприклад, AWS CloudFormation дозволяє визначати інфраструктуру як код (Infrastructure as Code), що спрощує створення та підтримку складних хмарних середовищ. Завдяки цьому інструменту організації можуть зменшити час, необхідний для розгортання нових проєктів, і мінімізувати ризики, пов'язані з людськими помилками.



Рисунок 2.1 – Діаграма архітектури AWS

Моніторинг і керування ресурсами забезпечуються через такі сервіси, як Amazon CloudWatch, який відстежує стан обчислювальних ресурсів, трафік, продуктивність додатків та інші метрики в реальному часі. Це дозволяє оперативно реагувати на потенційні проблеми, наприклад, підвищення навантаження на сервери або відхилення в роботі систем. AWS також пропонує інструменти автоматичного масштабування (Auto Scaling), які дозволяють динамічно

адаптувати ресурси до змінних потреб, забезпечуючи стабільність і ефективність роботи додатків.

Важливою складовою є підтримка гібридних та мультихмарних середовищ. AWS надає сервіси, які дозволяють інтегрувати її ресурси з іншими хмарними платформами або локальними дата-центрами. Наприклад, AWS Outposts дозволяє розгортати ресурси AWS безпосередньо в локальних дата-центрах, забезпечуючи сумісність і узгодженість із хмарними сервісами. Це особливо актуально для організацій, які потребують низької затримки доступу до даних або працюють у секторах із суворими вимогами до зберігання даних.

Архітектура AWS також орієнтована на забезпечення стійкості до збоїв. Завдяки розподіленій інфраструктурі, яка охоплює десятки регіонів і сотні зон доступності, AWS гарантує безперервність роботи навіть у випадку серйозних технічних збоїв. Використання механізмів резервування, дублювання даних і автоматичного відновлення сприяє підвищенню надійності систем [10].

Крім того, архітектура AWS активно підтримує впровадження сучасних технологій, таких як контейнери та серверлесс-обчислення. Наприклад, сервіси Amazon ECS (Elastic Container Service) та Amazon EKS (Elastic Kubernetes Service) забезпечують ефективну оркестрацію контейнеризованих додатків, що дозволяє розробникам швидше створювати, тестувати та розгортати додатки. Серверлесс-підхід, який реалізується через AWS Lambda, дозволяє виконувати код у відповідь на події без необхідності управління інфраструктурою, що значно скорочує витрати на підтримку систем.

Іншим важливим аспектом є аналітичні можливості AWS. Сервіси, такі як Amazon Athena, Amazon Redshift і AWS Glue, дозволяють організаціям працювати з великими обсягами даних, виконуючи складні аналітичні обчислення та отримуючи цінні інсайти для прийняття рішень. Інтеграція цих сервісів із системами машинного навчання, такими як Amazon SageMaker, відкриває нові горизонти для автоматизації бізнес-процесів і створення інноваційних продуктів. Архітектура AWS є прикладом сучасного підходу до побудови хмарних платформ, який поєднує інновації, стабільність, безпеку та масштабованість. Її гнучкість

дозволяє задовольнити різноманітні потреби користувачів, незалежно від галузі чи розміру організації, створюючи нові можливості для ефективного використання інформаційних технологій [11].

2.2 Архітектура платформи Eucalyptus

Архітектура платформи Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems) є децентралізованою системою, яка забезпечує можливість створення приватних хмарних середовищ. Вона побудована таким чином, щоб забезпечити гнучкість, масштабованість і сумісність із публічними хмарами, зокрема з Amazon Web Services (AWS). Eucalyptus надає користувачам можливість керувати обчислювальними ресурсами, мережами та сховищами даних, використовуючи стандартизовані API, що дозволяє інтегрувати локальні хмарні середовища з публічними хмарами.

Основою архітектури Eucalyptus є її модульна структура, яка складається з декількох ключових компонентів, кожен з яких виконує певну функцію. Головним компонентом є Cloud Controller (CLC), який забезпечує загальне управління хмарою. Цей модуль відповідає за взаємодію з іншими компонентами, обробку запитів від користувачів, а також управління ресурсами хмари. Cloud Controller забезпечує інтерфейс API, сумісний із AWS, що дозволяє користувачам легко використовувати сервіси, аналогічні до Amazon EC2, S3 тощо.

Другим важливим елементом є Cluster Controller (CC), який координує роботу окремих кластерів у межах хмари. Кластери складаються з обчислювальних вузлів, які надають ресурси для запуску віртуальних машин. Cluster Controller керує трафіком між вузлами, обробляє запити на створення, зупинку чи зміну конфігурації віртуальних машин і забезпечує зв'язок із Cloud Controller. Ця ієрархічна структура дозволяє масштабувати систему, додаючи нові кластери у разі зростання потреб.

Node Controller (NC) є ще одним важливим елементом архітектури. Він розташований на кожному фізичному сервері та відповідає за управління віртуальними машинами, що працюють на цьому сервері. Node Controller

забезпечує виконання команд, отриманих від Cluster Controller, таких як створення або зупинка віртуальних машин, а також моніторинг стану фізичних ресурсів, таких як процесори, пам'ять і диски. Система зберігання даних в Eucalyptus забезпечується за допомогою Storage Controller (SC) та Walrus Storage Service. Storage Controller відповідає за управління блочними сховищами даних, які використовуються віртуальними машинами. Walrus Storage Service забезпечує зберігання об'єктів, аналогічно до Amazon S3, і дозволяє користувачам зберігати файли, архіви чи інші типи даних. Ці сервіси забезпечують високий рівень доступності та інтеграцію з іншими компонентами системи. Мережевий рівень Eucalyptus реалізовано через Networking Controller (NC), який відповідає за створення, налаштування та управління мережами, що використовуються віртуальними машинами. Networking Controller дозволяє налаштовувати приватні та публічні IP-адреси, створювати ізольовані мережеві середовища та забезпечувати безпечний доступ до ресурсів [12].

Безпека в архітектурі Eucalyptus забезпечується через механізми аутентифікації та авторизації, які інтегровані в кожен компонент. Eucalyptus використовує стандартні протоколи безпеки, такі як SSL, для захисту даних, а також дозволяє застосовувати політики доступу на основі ролей, що дозволяє адміністраторам керувати доступом до ресурсів. Особливістю архітектури Eucalyptus є її орієнтація на інтеграцію з AWS. Наприклад, API Eucalyptus повністю сумісний із API AWS, що дозволяє користувачам легко переміщувати робочі навантаження між приватними і публічними хмарами. Це робить Eucalyptus ідеальним вибором для організацій, які прагнуть зберігати контроль над конфіденційними даними, але водночас хочуть скористатися перевагами публічних хмар для масштабування.

Продовжуючи аналіз архітектури платформи Eucalyptus, важливо звернути увагу на її ключову перевагу — адаптивність до різних середовищ. Завдяки модульному дизайну, кожен компонент Eucalyptus може бути налаштований окремо, що дозволяє створювати індивідуальні рішення для специфічних потреб організації. Це означає, що компанія може використовувати тільки ті компоненти,

які потрібні для її роботи, зменшуючи загальну складність системи та витрати на її підтримку.

Інтеграція з іншими системами — ще одна сильна сторона Eucalyptus. Платформа підтримує стандартизовані інтерфейси, що дозволяє підключати стороннє програмне забезпечення для управління обчислювальними ресурсами, моніторингу, резервного копіювання або автоматизації процесів. Це забезпечує високу гнучкість, особливо для організацій, які вже мають власні інструменти для управління IT-інфраструктурою. Для підвищення ефективності використання ресурсів Eucalyptus підтримує механізми автоматичного масштабування, які дозволяють динамічно розподіляти обчислювальні навантаження між вузлами в кластері. Наприклад, у пікові періоди платформа може автоматично збільшувати кількість віртуальних машин, а після завершення навантаження — звільняти невикористані ресурси. Це робить Eucalyptus економічно вигідним рішенням для організацій, що працюють з нерівномірними навантаженнями.

Щодо забезпечення безперервності роботи, архітектура Eucalyptus використовує принципи резервування. Наприклад, якщо один із фізичних серверів або кластерів виходить з ладу, платформа автоматично перенаправляє завдання на інші доступні ресурси. Це значно знижує ризик збоїв і забезпечує високу доступність послуг навіть у випадку непередбачених технічних проблем.

Ще однією унікальною особливістю є відкритий код Eucalyptus. Це дозволяє організаціям не лише використовувати платформу, але й модифікувати її під свої потреби. Відкритість коду робить Eucalyptus привабливим для наукових та дослідницьких установ, які часто потребують специфічних рішень, недоступних у комерційних хмарах [13].

Перспективи розвитку Eucalyptus також пов'язані з впровадженням нових технологій, таких як контейнеризація та оркестрація контейнерів. Наприклад, інтеграція з Kubernetes або Docker може значно розширити можливості Eucalyptus у сфері розробки та розгортання сучасних додатків. Крім того, активна розробка API, сумісних із іншими провідними платформами, такими як Google Cloud або

Microsoft Azure, відкриває нові горизонти для використання Eucalyptus у гібридних і мультіхмарних середовищах.

Архітектура Eucalyptus також характеризується високою надійністю та ефективністю використання ресурсів. Завдяки підтримці механізмів автоматичного масштабування система динамічно адаптується до змін у навантаженні. Наприклад, у разі збільшення потреб у ресурсах Eucalyptus може автоматично запускати додаткові віртуальні машини для обслуговування нових запитів. Водночас, при зниженні навантаження платформа вивільняє невикористані ресурси, що сприяє зменшенню витрат на їх утримання. На рисунку 2.2 зображена архітектура системи Eucalyptus.

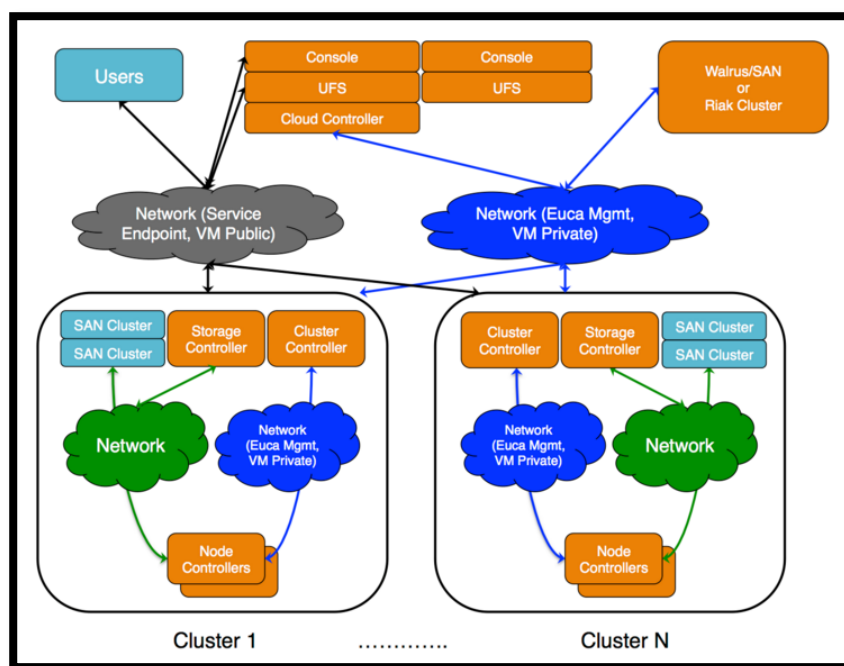


Рисунок 2.2 – Діаграма архітектури

Для забезпечення безперервності роботи архітектура Eucalyptus використовує принципи резервування. Якщо один із фізичних серверів або кластерів виходить з ладу, система автоматично перенаправляє робочі навантаження на інші доступні ресурси. Це дозволяє уникнути простоїв та мінімізує ризик втрати даних чи відмови сервісів. Такий підхід особливо важливий для критичних додатків, де висока доступність є ключовою вимогою.

Ще однією важливою перевагою Eucalyptus є її здатність інтегруватися з існуючою IT-інфраструктурою завдяки використанню стандартизованих API. Це дозволяє організаціям без зусиль інтегрувати платформу у свої процеси та використовувати стороннє програмне забезпечення для моніторингу, автоматизації, резервного копіювання чи управління обчислювальними ресурсами. Така гнучкість робить Eucalyptus особливо привабливою для організацій зі складною інфраструктурою, яка вже існує.

Крім того, відкритий код Eucalyptus дозволяє розробникам і дослідникам створювати індивідуальні рішення для конкретних потреб. Завдяки цьому платформа знайшла своє застосування в академічному середовищі, де часто потрібна модифікація інструментів для проведення досліджень або розробки інноваційних продуктів [14].

Важливим аспектом розвитку Eucalyptus є її інтеграція з новітніми технологіями, такими як контейнеризація та оркестрація. Наприклад, впровадження підтримки Kubernetes чи Docker дозволяє використовувати платформу для управління контейнерними додатками, що робить її ще більш універсальною. Окрім цього, розширення підтримки API для інших хмарних платформ, таких як Google Cloud чи Microsoft Azure, сприяє створенню гібридних і мультіхмарних рішень, що забезпечують максимальну гнучкість для користувачів.

Серед інших переваг варто виділити підхід до безпеки в Eucalyptus. Інтегровані механізми аутентифікації та авторизації дозволяють забезпечувати надійний контроль доступу до ресурсів і захист даних від несанкціонованого доступу. Завдяки використанню стандартів безпеки, таких як SSL, платформа гарантує конфіденційність та цілісність переданої інформації. Політики доступу на основі ролей дають адміністраторам змогу ефективно керувати доступом до різних компонентів системи.

Архітектура платформи Eucalyptus також демонструє високу ефективність у контексті управління великими обчислювальними навантаженнями завдяки її здатності до автоматизованого управління ресурсами. Цей підхід передбачає не

лише оптимальний розподіл навантаження між вузлами, а й інтеграцію з технологіями моніторингу. Постійний контроль за використанням ресурсів дозволяє системі вчасно реагувати на зміни у вимогах, що особливо важливо для підприємств, які працюють із критично важливими даними або додатками з високою інтенсивністю використання.

Окрім цього, Eucalyptus активно впроваджує нові механізми оркестрації, що дає змогу забезпечувати плавність у роботі навіть за умови пікових навантажень. Наприклад, у разі різкого збільшення кількості запитів платформа автоматично ініціює процес створення додаткових обчислювальних вузлів, які після завершення навантаження можуть бути автоматично звільнені, забезпечуючи економію ресурсів.

Інтеграція з існуючими екосистемами залишається однією з ключових переваг Eucalyptus. Завдяки модульному підходу платформа може бути налаштована для роботи з будь-якими системами управління, які вже використовуються у компанії. Це дає змогу скоротити час адаптації до нової інфраструктури та зменшити витрати, пов'язані з переходом на іншу систему. Висока сумісність із API інших хмарних платформ також дозволяє організаціям гнучко керувати своїми хмарними середовищами, інтегруючи приватні ресурси з публічними для досягнення максимальної ефективності.

Безпека залишається пріоритетом в архітектурі Eucalyptus. Використання сучасних криптографічних протоколів і технологій шифрування даних дозволяє забезпечити не лише захист інформації від несанкціонованого доступу, а й її цілісність під час передачі між компонентами. Особливої уваги заслуговує можливість застосування політик доступу, які ґрунтуються на ролях, що дозволяє чітко розподіляти права доступу до ресурсів, враховуючи рівень відповідальності користувачів.

Завдяки високій адаптивності та можливостям кастомізації Eucalyptus ідеально підходить для широкого спектра застосувань, включаючи корпоративні середовища, дослідницькі установи та освітні заклади. Наприклад, компанії можуть використовувати Eucalyptus для побудови приватних хмарних платформ,

які інтегруються з публічними хмарами для масштабування обчислювальних потужностей у разі необхідності. Водночас дослідницькі організації можуть адаптувати відкритий код платформи для створення спеціалізованих рішень, що відповідають їхнім унікальним завданням.

З точки зору перспектив розвитку, важливо зазначити, що платформа продовжує вдосконалюватися, інтегруючи нові технології, такі як штучний інтелект і машинне навчання. Це дозволяє не лише оптимізувати процеси управління ресурсами, а й впроваджувати передові рішення для автоматизації рутинних операцій. Крім того, посилена підтримка технологій контейнеризації, таких як Kubernetes, відкриває нові горизонти для розробників, забезпечуючи їм додаткові можливості для створення і розгортання складних додатків у гнучких і динамічних середовищах.

Таким чином, Eucalyptus залишається універсальним і перспективним інструментом для організацій, які прагнуть ефективно використовувати свої ресурси, забезпечуючи при цьому високий рівень безпеки, гнучкості та надійності. Її здатність до інтеграції, масштабування та адаптації під специфічні потреби користувачів робить платформу ідеальним вибором для вирішення завдань будь-якої складності [15].

2.3 Інструменти та методи інтеграції

Інструменти та методи інтеграції в хмарних середовищах відіграють ключову роль у забезпеченні узгодженої роботи різних компонентів ІТ-інфраструктури, оптимізації ресурсів і підвищенні ефективності бізнес-процесів. Інтеграція дозволяє поєднувати локальні та хмарні ресурси, забезпечувати взаємодію між різними хмарними платформами та створювати гібридні середовища. Для цього використовуються різноманітні інструменти та методи, орієнтовані на досягнення високої продуктивності, безпеки та масштабованості.

Одним із найважливіших методів інтеграції є використання API (Application Programming Interface). API забезпечує стандартизований інтерфейс для взаємодії між додатками, сервісами та платформами. Наприклад, хмарні платформи, такі як

AWS або Eucalyptus, надають свої API, які дозволяють автоматизувати управління обчислювальними ресурсами, налаштування мереж або зберігання даних. Це дозволяє організаціям створювати власні додатки, що інтегруються з хмарними середовищами, або використовувати сторонні рішення для управління ресурсами.

Іншим важливим інструментом інтеграції є оркестратори, такі як Kubernetes або Docker Swarm. Вони дозволяють керувати контейнеризованими додатками, автоматизуючи розгортання, масштабування та балансування навантаження. Оркестратори забезпечують єдиний шар управління для додатків, що працюють у різних середовищах, включаючи публічні та приватні хмари. Це спрощує процес інтеграції та підвищує стійкість додатків до збоїв.

Для інтеграції локальних і хмарних середовищ активно використовуються технології гібридних хмар. Наприклад, AWS Outposts дозволяє розгорнути хмарні ресурси AWS безпосередньо у локальних дата-центрах, що забезпечує безшовну інтеграцію з глобальною інфраструктурою AWS. Це рішення особливо корисне для організацій, які мають суворі вимоги до зберігання даних або працюють у регіонах із високими вимогами до затримки.

Методи інтеграції часто включають використання сервісів передачі даних, таких як Amazon S3 Transfer Acceleration або Azure Data Box. Ці інструменти забезпечують швидку та безпечну передачу великих обсягів даних між локальними середовищами та хмарними платформами. Такі сервіси також підтримують шифрування даних, що забезпечує їхню безпеку під час передачі.

Для забезпечення узгодженої роботи додатків у мультихмарних середовищах використовуються рішення для управління хмарною інфраструктурою, наприклад, Terraform. Це інструмент, який дозволяє визначати інфраструктуру як код (Infrastructure as Code), автоматизуючи розгортання та налаштування ресурсів у різних хмарах. Terraform підтримує широкий спектр хмарних платформ, що дозволяє легко інтегрувати їх у загальну ІТ-екосистему.

Методи інтеграції також включають використання сервісних шин даних (Service Bus), таких як Azure Service Bus або Apache Kafka. Ці інструменти забезпечують надійну передачу повідомлень між різними компонентами системи,

незалежно від їхньої географічної розташованості або платформи, на якій вони працюють. Сервісні шини дозволяють синхронізувати роботу додатків, забезпечуючи їхню узгоджену взаємодію.

Особливе значення мають інструменти для моніторингу та управління інтеграцією. Наприклад, платформи, такі як AWS CloudWatch або Google Cloud Operations Suite, дозволяють відстежувати стан хмарних ресурсів, аналізувати трафік і оперативно виявляти проблеми. Це забезпечує стабільність роботи інтегрованих систем і знижує ризик простоїв. Інструменти та методи інтеграції є невід'ємною частиною сучасних хмарних обчислень. Вони дозволяють забезпечити узгоджену роботу різних компонентів IT-інфраструктури, спрощують управління ресурсами та відкривають нові можливості для бізнесу. Ефективна інтеграція вимагає ретельного вибору інструментів і методів, які відповідають специфічним потребам організації. У контексті інтеграції важливим аспектом є забезпечення безпеки під час передачі даних та взаємодії між компонентами різних систем. Інструменти та методи інтеграції мають враховувати ризики, пов'язані з несанкціонованим доступом, перехопленням інформації або компрометацією даних під час їх передачі. Для цього використовуються механізми шифрування, автентифікації та авторизації.

Шифрування даних під час інтеграції забезпечується за допомогою таких протоколів, як TLS (Transport Layer Security) або IPSec (Internet Protocol Security). Ці технології створюють захищені канали для передачі даних, які гарантують, що інформація не буде доступна для сторонніх осіб навіть у разі її перехоплення. Наприклад, у хмарних середовищах TLS використовується для забезпечення безпеки API-запитів між локальними системами та хмарними сервісами.

Автентифікація користувачів і систем є ще одним важливим елементом інтеграції. Інструменти, такі як AWS IAM (Identity and Access Management) або Azure Active Directory, дозволяють керувати доступом до ресурсів, забезпечуючи багатофакторну автентифікацію. Це дозволяє організаціям забезпечувати доступ до інтегрованих систем лише уповноваженим користувачам або додаткам.

Авторизація базується на політиках доступу, які визначають, що саме може робити конкретний користувач або сервіс у межах інтегрованої системи. Наприклад, у платформі AWS можна створювати детальні політики, які обмежують дії користувачів або додатків, знижуючи ризики випадкових або зловмисних змін у хмарних ресурсах.

Ще одним ключовим аспектом інтеграції є забезпечення сумісності між різними платформами та системами. У цьому контексті стандартизація відіграє важливу роль. Наприклад, використання стандартних протоколів, таких як REST або SOAP, дозволяє забезпечити взаємодію між додатками, незалежно від технологій, на яких вони побудовані. Це спрощує інтеграцію і знижує залежність від конкретного постачальника.

Управління конфігураціями є ще одним важливим методом інтеграції. Інструменти, такі як Ansible, Puppet або Chef, дозволяють автоматизувати налаштування систем і забезпечувати їхню узгодженість у різних середовищах. Це особливо корисно в масштабних хмарних системах, де навіть невеликі помилки в конфігураціях можуть призвести до серйозних збоїв.

Для підтримки стабільності інтегрованих систем важливим є використання інструментів для відновлення після збоїв. Наприклад, сервіси резервного копіювання, такі як AWS Backup або Azure Backup, дозволяють зберігати копії даних і конфігурацій, забезпечуючи швидке відновлення роботи у разі технічних проблем. Це мінімізує ризики втрати даних або простоїв у роботі систем. Нарешті, у сучасних умовах інтеграція повинна враховувати потреби в масштабуванні систем. Динамічне масштабування, яке підтримується більшістю хмарних платформ, дозволяє автоматично збільшувати або зменшувати обсяги ресурсів залежно від поточного навантаження. Це забезпечує ефективне використання ресурсів та стабільну роботу інтегрованих систем навіть під час пікових навантажень. В таблиці 2.1 відображені доступні методи інтеграції двох систем.

Таблиця 2.1 Інструменти та методи інтеграції для AWS та Eucalyptus

Характеристика	AWS	Eucalyptus
Тип інтеграції	Інтеграція через API, серверлесс, гібридні хмари	Інтеграція через API, локальні хмари, сумісність з AWS
Інструменти для передачі даних	AWS S3 Transfer Acceleration, AWS Direct Connect	Eucalyptus Storage, Walrus Storage Service, VPN
Методи безпеки	Шифрування, багатофакторна аутентифікація, IAM, SSL	Шифрування, SSL, ролі доступу
Інструменти для моніторингу	Amazon CloudWatch, AWS X-Ray	Eucalyptus CloudWatch, OpenStack Monasca
Масштабування	Автоматичне масштабування, EC2 Auto Scaling, Lambda	Масштабування залежно від локальних ресурсів
Інтеграція з іншими системами	Інтеграція з AWS, сторонніми сервісами через API	Сумісність з AWS API, обмежена інтеграція з іншими платформами
Керування доступом	IAM, багатофакторна аутентифікація, політики доступу	Керування через ролі доступу, контроль на рівні адміністратора

Таким чином, інтеграція в сучасних хмарних середовищах — це не лише технічний процес, а й стратегічний підхід до побудови надійних, безпечних і масштабованих систем. Використання правильних інструментів і методів дозволяє організаціям досягати високої продуктивності, мінімізувати ризики та забезпечувати гнучкість у впровадженні нових технологій.

3 РОЗРОБКА МОДЕЛІ ІНТЕГРОВАНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

3.1 Постановка задачі проектування

Проектування інтегрованої мережевої інфраструктури є складним і багатогранним завданням, яке вимагає ретельного підходу до вибору компонентів, їхньої взаємодії, а також забезпечення високої ефективності, масштабованості та безпеки всієї системи. Постановка задачі проектування інтегрованої мережевої інфраструктури передбачає не тільки врахування технічних аспектів, а й стратегічних цілей організації, забезпечення безперервності бізнес-процесів та максимізації ресурсної ефективності.

Основною метою проектування є створення мережевої інфраструктури, яка здатна задовольнити вимоги до обчислювальної потужності, зберігання даних, мережевого трафіку та обміну даними між різними компонентами системи. Це означає, що на етапі постановки задачі необхідно визначити обсяг і типи даних, що будуть передаватися через мережу, вимоги до швидкості обробки, надійності і доступності, а також прогнозовані навантаження на систему в умовах змінюваного або зростаючого попиту.

Одним із ключових аспектів є інтеграція локальних, гібридних і публічних хмарних середовищ. Мережа повинна забезпечувати безперебійну взаємодію між різними типами інфраструктури — від локальних дата-центрів до публічних хмарних платформ, таких як AWS або Microsoft Azure. Водночас необхідно врахувати особливості мережевого з'єднання, включаючи використання VPN, проксі-серверів, а також технології балансування навантаження для забезпечення рівномірного розподілу трафіку і підтримки високої доступності.

Завдання проектування мережі включає вибір правильних мережевих протоколів, розробку схем маршрутизації, вибір правильного обладнання, яке буде використовуватися для підключення серверів і робочих станцій до мережі. Особливу увагу потрібно приділяти вибору обладнання для побудови надійної та швидкої інфраструктури, такої як комутатори, маршрутизатори, мережеві шлюзи та системи для моніторингу мережі [16].

Проектування також передбачає розробку стратегії безпеки для захисту від несанкціонованого доступу, зловмисних атак та витоку даних. Задача безпеки є критично важливою, оскільки інформація, що передається по мережі, може бути конфіденційною або містити інтелектуальну власність компанії. Використання шифрування, створення багаторівневих систем захисту, впровадження політик контролю доступу, багатофакторної автентифікації і забезпечення стійкості до атак типу DDoS є необхідними умовами для побудови надійної мережевої інфраструктури.

Крім того, в процесі постановки задачі важливо визначити критерії ефективності мережі. Це включає не тільки фізичні і логічні параметри, такі як швидкість передачі даних, але й забезпечення масштабованості та адаптивності системи до змінюваних вимог. У зв'язку з цим проектування мережі повинно передбачати використання технологій автоматичного масштабування, інтеграції з системами керування ресурсами та балансування навантаження.

Завдання проектування також включає створення стратегії для обробки великих обсягів даних, управління трафіком та забезпечення високої швидкості обробки запитів у реальному часі. Для цього може бути застосована технологія кешування, а також використання швидких каналів зв'язку і оптимізованих протоколів для зменшення часу затримки при передаванні даних.

На заключному етапі проектування, необхідно розробити план впровадження та тестування мережевої інфраструктури, що включає перевірку працездатності мережі в умовах реального навантаження, виявлення можливих уразливих місць і неполадок, а також підготовку заходів для їхнього усунення. Тестування повинно охоплювати різні сценарії роботи системи, від звичайного користувацького трафіку до пікових навантажень. Проектування інтегрованої мережевої інфраструктури також вимагає ретельного планування її підтримки в довгостроковій перспективі. Це включає визначення процедур для оновлення, модифікації та вдосконалення мережі, що повинні забезпечувати безперервність бізнес-процесів і зниження ризиків, пов'язаних з застарілим обладнанням або програмним забезпеченням. Одним із важливих аспектів є моніторинг стану мережі та її компонентів. Це

дозволяє оперативно виявляти проблеми та забезпечувати своєчасну реакцію на будь-які несправності або збої, що можуть вплинути на працездатність системи. Впровадження систем моніторингу та управління ресурсами дозволяє забезпечити стабільність роботи мережі навіть при зростанні навантажень або зміні умов використання.

Важливим етапом є також планування і тестування відновлення після збоїв. Необхідно створити стратегію аварійного відновлення, яка визначає порядок дій при збої в одній з частин мережі, а також визначає методи відновлення критичних даних та сервісів. Це забезпечує безперервність роботи і мінімізує час, коли система не функціонує. Розробка плану аварійного відновлення також передбачає регулярне тестування всіх компонентів системи, щоб переконатися в їхній готовності до роботи у випадку непередбачених ситуацій. Проектування мережевої інфраструктури має також враховувати вимоги до енергетичної ефективності та екологічної стійкості. Зниження енергоспоживання без втрати продуктивності стало важливим аспектом у проектуванні сучасних ІТ-систем. Для цього можуть бути застосовані енергозберігаючі технології, такі як оптимізація використання серверів, використання віртуалізації для більш ефективного розподілу ресурсів та інтеграція з відновлюваними джерелами енергії. Це не тільки знижує витрати на обслуговування інфраструктури, а й підвищує загальну ефективність і стійкість бізнесу.

Усе це вимагає інтеграції між різними підсистемами та технологіями, що забезпечують функціонування мережі, як зображено на рисунку 3.1, а також тісної взаємодії між адміністраторами мереж і іншими відділами організації. Спільна робота дозволяє досягати найкращих результатів, сприяє швидкому вирішенню проблем і покращує взаємодію між бізнес-цілями і технічними аспектами проектування.

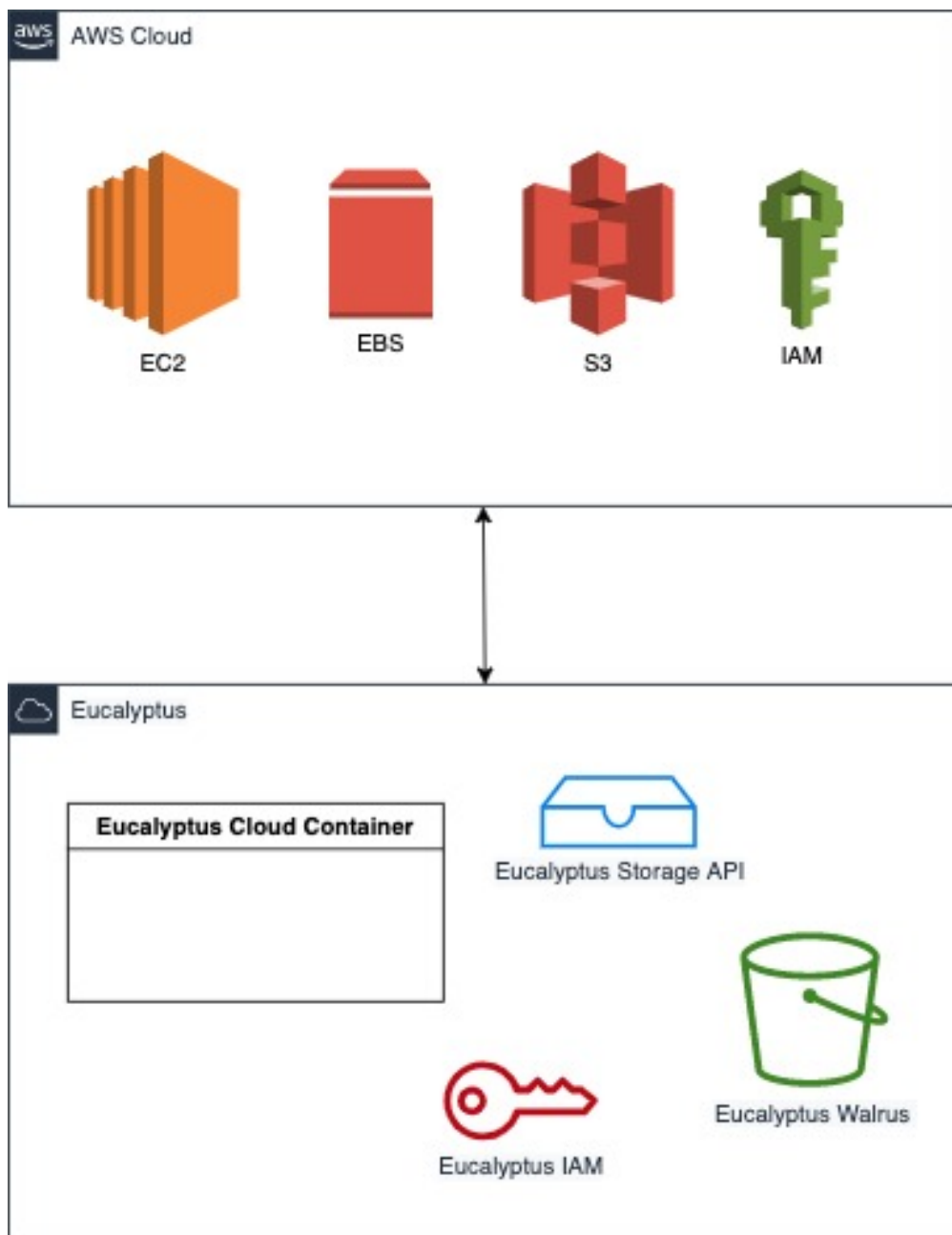


Рисунок 3.1 – Діаграма проектування інтегрованої мережевої інфраструктури

У завершенні, проектування інтегрованої мережевої інфраструктури має не тільки технічні, а й стратегічні вимоги. Воно повинно враховувати майбутні потреби бізнесу, новітні технології, вимоги до безпеки і збереження даних, а також забезпечувати можливість безперервного вдосконалення та адаптації до нових умов. Ретельно сплановане проектування створює основу для надійної, масштабованої і безпечної мережі, що відповідає вимогам організації і здатна підтримувати її бізнес-процеси на високому рівні.

3.2 Вибір програмного забезпечення та інструментів

Вибір програмного забезпечення та інструментів для проектування та реалізації мережевої інфраструктури є ключовим етапом у процесі побудови ефективної, надійної та безпечної системи. Правильний вибір програмних рішень дозволяє забезпечити оптимальне використання ресурсів, мінімізувати ризики, підвищити продуктивність і забезпечити безперебійну роботу мережі. Це складне завдання, яке включає багато аспектів, зокрема сумісність з іншими системами, масштабованість, безпека, підтримка нових технологій і надійність.

Одним з основних критеріїв вибору програмного забезпечення є його здатність інтегруватися з іншими інструментами, які вже використовуються в організації або які планується впровадити в майбутньому. Наприклад, в сучасних умовах часто потрібна інтеграція з хмарними платформами, такими як AWS, Microsoft Azure або Google Cloud, тому вибір інструментів повинен забезпечувати сумісність з API цих платформ, а також підтримку гібридних і мультіхмарних середовищ. Інструменти, які пропонують API, що сумісні з іншими хмарними сервісами, дозволяють легко масштабувати інфраструктуру та інтегрувати її з іншими компонентами системи.

Завдання вибору програмного забезпечення також передбачає розгляд можливості автоматизації процесів управління мережею. Оскільки ефективність роботи мережі залежить від швидкості реагування на зміни в навантаженні, наявність інструментів для автоматичного масштабування і балансування навантаження є важливою вимогою. Для цього можуть бути використані такі платформи, як Kubernetes або Docker Swarm, які автоматизують оркестрацію контейнеризованих додатків і дозволяють забезпечити безшовну інтеграцію з іншими компонентами системи. Такі інструменти значно знижують необхідність ручного втручання, що робить процес управління мережею більш ефективним і менш схильним до помилок.

Ще одним важливим аспектом вибору програмного забезпечення є забезпечення високої безпеки. Оскільки мережі часто є основними точками доступу до конфіденційної інформації, вибір інструментів для забезпечення

безпеки даних, захисту від несанкціонованого доступу і виявлення загроз є критичним. Програмне забезпечення повинно включати функції шифрування, аутентифікації та моніторингу, а також інтегруватися з системами управління інцидентами безпеки (SIEM). Інструменти, такі як AWS Identity and Access Management (IAM) або Microsoft Azure Active Directory, дозволяють налаштовувати доступ до ресурсів на основі ролей і політик, що забезпечує захист мережі на різних рівнях.

Масштабованість програмного забезпечення є ще одним важливим критерієм. Оскільки зростання вимог до мережевих ресурсів неминуче, програмне забезпечення повинно мати можливість підтримувати високу продуктивність і стабільність при збільшенні навантаження. Наприклад, використання програмних рішень для моніторингу і керування ресурсами, таких як Amazon CloudWatch або Zabbix, дозволяє в реальному часі відстежувати стан мережі та ресурси, щоб своєчасно виявляти перевантаження і вживати відповідних заходів.

Вибір програмного забезпечення також пов'язаний з необхідністю забезпечення високої доступності та стійкості до збоїв. У разі відмови одного з компонентів мережі або в умовах технічних проблем, програмні рішення повинні передбачати механізми відновлення після збоїв, такі як автоматичне переключення на резервні вузли або використання резервних копій даних. Інструменти для аварійного відновлення, такі як AWS Backup або Veeam, дозволяють швидко відновити дані і систему у разі збоїв, мінімізуючи час простою. Також важливою складовою вибору програмного забезпечення є його відповідність стандартам і нормативам, що застосовуються до конкретної галузі. Наприклад, організації, що працюють в сфері фінансів або охорони здоров'я, повинні вибирати програмні інструменти, які відповідають вимогам законодавства щодо зберігання і обробки персональних даних, таким як GDPR або HIPAA.

Вибір програмного забезпечення не обмежується лише функціональністю, безпекою або сумісністю з іншими інструментами. Важливим аспектом є підтримка постійних оновлень і покращень, а також можливість розширення функціоналу в майбутньому. Оскільки технології постійно розвиваються, програмне забезпечення

повинно бути адаптованим до нових стандартів і тенденцій, щоб не стати застарілим у короткий час.

Вибір програмного забезпечення та інструментів для проектування і управління мережею є важливим процесом, який вимагає детального аналізу та врахування безлічі факторів, від безпеки і масштабованості до інтеграції з іншими системами. Тільки правильне поєднання цих факторів дозволяє створити ефективну та надійну мережеву інфраструктуру, яка задовольняє вимоги бізнесу та забезпечує стабільність роботи всіх компонентів системи. Оскільки мережеві технології постійно еволюціонують, вибір програмного забезпечення також має включати можливість інтеграції нових технологій і адаптації до майбутніх змін. Важливим аспектом є підтримка таких технологій, як віртуалізація, контейнеризація та оркестрація, які вже стали стандартом для більшості хмарних та корпоративних мереж. Програмне забезпечення повинно бути здатним ефективно працювати з платформами для віртуалізації, такими як VMware або Microsoft Hyper-V, а також підтримувати контейнерні технології, такі як Docker і Kubernetes. Це дозволяє забезпечити гнучкість і швидкість розгортання додатків, а також оптимізувати використання мережевих ресурсів.

Інтеграція з аналітичними інструментами та платформами для великих даних також є важливим аспектом вибору програмного забезпечення. Більшість сучасних мереж генерують величезні обсяги даних, що потребують аналізу для виявлення тенденцій, підвищення ефективності або виявлення аномалій, які можуть свідчити про безпекові загрози. Вибір програмного забезпечення, яке підтримує інтеграцію з такими інструментами, як Apache Hadoop, Apache Spark або інші платформи для обробки великих даних, дозволяє забезпечити кращу видимість і контроль над роботою мережі. Це дає змогу приймати обґрунтовані рішення на основі реальних даних і передбачати потенційні проблеми до їх виникнення.

Іншим важливим аспектом є вибір програмного забезпечення, яке підтримує автоматизацію операцій. Враховуючи швидкий розвиток і ускладнення мереж, управління ними вимагає постійного втручання, що може бути обтяжливим для ІТ-спеціалістів. Вибір інструментів для автоматизації, таких як Ansible, Puppet або

Chef, допомагає оптимізувати управлінські процеси, знижуючи кількість ручних налаштувань і забезпечуючи швидке реагування на зміни у навантаженні або структурі мережі. Завдяки автоматизації адміністрування стає більш ефективним, а також зменшується кількість людських помилок, що можуть виникати в процесі налаштування чи моніторингу мережі. В таблиці 3.1 більш детально розглянуті критерії вибору програмного забезпечення та інструментів.

Таблиця 3.1 Критерії вибору програмного забезпечення та інструментів для AWS та Eucalyptus

Критерії вибору	AWS	Eucalyptus
Тип інфраструктури	Публічна хмара з можливістю гібридної інтеграції	Приватна хмара, сумісність з AWS API
Інтеграція з хмарними платформами	Сумісність з AWS, інтеграція з іншими хмарами через API	Інтеграція з AWS API, обмежена інтеграція з іншими платформами
Масштабованість	Висока масштабованість через автоматичне масштабування та балансування навантаження	Масштабованість залежить від локальних ресурсів
Безпека	Високий рівень безпеки (шифрування, IAM, багатофакторна аутентифікація)	Можливість налаштування безпеки на рівні локальної інфраструктури
Автоматизація процесів	Підтримка автоматизації через сервіси AWS CloudFormation та Lambda	Автоматизація через OpenStack та інші інструменти для локальних хмар

Продовження таблиці 3.1 Критерії вибору програмного забезпечення та інструментів для AWS та Eucalyptus

Інструменти для моніторингу	Моніторинг через Amazon CloudWatch і X-Ray	Моніторинг через Eucalyptus CloudWatch, OpenStack Monasca
Інструменти для резервного копіювання	Резервне копіювання через AWS Backup	Резервне копіювання через сторонні інструменти або локальні рішення
Підтримка віддаленої роботи	Підтримка віддаленої роботи через VPN і AWS WorkSpaces	Підтримка віддаленої роботи через VPN та інші локальні інструменти
Інтеграція з іншими системами	Інтеграція з іншими хмарними платформами та локальними системами через API	Сумісність з AWS API, обмежена інтеграція з іншими хмарами
Вартість	Моделі оплати на основі використання, що дозволяє знизити витрати	Вища вартість через необхідність створення власної інфраструктури

Не менш важливим є вибір програмного забезпечення для захисту від кіберзагроз. У сучасному світі кібербезпека є однією з головних проблем для будь-якої організації, тому вибір засобів для захисту мережевої інфраструктури є важливим етапом у процесі проектування. Інструменти, такі як брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS), а також рішення для шифрування даних, мають бути інтегровані в архітектуру мережі для забезпечення її безпеки. Вибір програмного забезпечення для моніторингу загроз і управління інцидентами (SIEM) дозволяє організації швидко виявляти і реагувати на загрози в реальному часі, зменшуючи ймовірність успішної атаки.

Для забезпечення високої доступності та надійності мережі також необхідно вибирати програмні рішення, які підтримують резервування та відновлення даних. Вибір інструментів для резервного копіювання та відновлення, таких як Veeam або

Commvault, дозволяє мінімізувати ризик втрати важливої інформації та забезпечити швидке відновлення після збою. Відновлення даних є критичним аспектом, особливо для організацій, що працюють з конфіденційною інформацією або критично важливими даними.

Забезпечення мобільності і підтримка віддаленої роботи також стають важливими аспектами вибору програмного забезпечення. Для забезпечення доступу до мережі з будь-якого місця необхідно використовувати інструменти для віртуальних приватних мереж (VPN), такі як OpenVPN або Cisco AnyConnect, які забезпечують безпечне підключення до мережі через Інтернет. Це дозволяє співробітникам працювати з будь-якої точки світу, зберігаючи високий рівень безпеки та контроль над доступом.

Отже, вибір програмного забезпечення та інструментів для мережевої інфраструктури є багатогранним процесом, що включає не тільки оцінку технічних характеристик, а й врахування потреб бізнесу, забезпечення безпеки, можливості автоматизації, інтеграції з іншими системами та підтримки майбутніх технологічних змін. Правильний вибір інструментів дозволяє створити гнучку, надійну та ефективну мережеву інфраструктуру, здатну підтримувати потреби організації в довгостроковій перспективі.

3.3 Модель інтеграції AWS та Eucalyptus

Модель інтеграції AWS та Eucalyptus передбачає поєднання можливостей двох платформ для створення високоефективної і масштабованої інфраструктури, яка поєднує як локальні ресурси, так і ресурси публічної хмари. Вона дозволяє використовувати найкраще з обох світів: контролювати важливі дані та ресурси в приватній хмарі, при цьому отримуючи переваги від масштабованості та гнучкості публічних хмарних платформ. Інтеграція між AWS та Eucalyptus здійснюється через використання спільних API та стандартів, що дозволяє забезпечити сумісність між цими платформами. Одним з головних аспектів цієї моделі є використання AWS API в Eucalyptus, що дозволяє розгорнути приватну хмару на базі Eucalyptus, яка зберігає сумісність з публічними хмарами AWS. Це забезпечує

безшовну інтеграцію між локальними хмарами та AWS, дозволяючи організаціям зберігати конфіденційність і контроль над даними, зберігаючи при цьому можливість масштабувати ресурси при потребі, використовуючи публічну хмару [17].

У рамках цієї моделі користувачі можуть створювати гібридні хмарні середовища, в яких Eucalyptus слугує як основна платформа для приватних хмар, а AWS використовується для розширення можливостей і додаткових обчислювальних потужностей. Наприклад, у разі пікових навантажень або необхідності в додаткових ресурсах для обробки великих даних, обчислювальні потужності можуть бути автоматично масштабовані шляхом інтеграції з AWS, де ресурси можуть бути додані без необхідності перепланування інфраструктури.

Інтеграція включає також механізми синхронізації даних між Eucalyptus та AWS. Для цього використовуються спеціальні сервіси, такі як Eucalyptus Walrus Storage Service, який забезпечує зберігання об'єктів, подібно до Amazon S3, що дозволяє зберігати великі обсяги даних у приватній хмарі, при цьому надаючи можливість для резервного копіювання або архівації в AWS. Це дозволяє створювати гнучкі стратегії резервного копіювання та відновлення даних, де частина даних зберігається локально, а частина — у публічній хмарі для підвищення доступності та безпеки.

Для забезпечення безперервної роботи і високої доступності важливою частиною інтеграції є механізми балансування навантаження та автоматичного масштабування. Наприклад, в AWS використовується Elastic Load Balancing (ELB), що дозволяє автоматично розподіляти трафік між інстанціями, що працюють у публічній хмарі, а в Eucalyptus подібна функціональність може бути реалізована через використання власних інструментів для балансування навантаження в приватних хмарах. У разі зростання навантаження, частина трафіку може бути направлена в AWS для обробки, забезпечуючи таким чином безперебійне функціонування системи.

Ще одним важливим аспектом інтеграції є управління безпекою та доступом. Використовуючи AWS Identity and Access Management (IAM) разом із системами

безпеки Eucalyptus, організації можуть забезпечити чітке управління доступом до ресурсів. Наприклад, користувачі можуть бути авторизовані для доступу до певних ресурсів у приватній хмарі Eucalyptus або у публічній хмарі AWS залежно від їхніх ролей і політик доступу. Завдяки цьому досягається високий рівень безпеки і контроль доступу до даних та ресурсів на обох платформах.

Крім того, інтеграція забезпечує підтримку резервування та відновлення після збоїв. Використовуючи механізми відновлення на обох платформах, можна створювати стратегії для аварійного відновлення даних і сервісів. Наприклад, у разі неполадок у приватній хмарі Eucalyptus, дані можуть бути автоматично перенесені до AWS, де вони будуть збережені і доступні для відновлення. Це дозволяє забезпечити безперервність бізнес-процесів, знизивши ризики втрати даних і збоїв у роботі систем.

Модель інтеграції AWS та Eucalyptus створює потужну основу для побудови гнучких і надійних хмарних рішень, які об'єднують переваги публічної та приватної хмарних платформ. Вона дозволяє організаціям створювати адаптивні інфраструктури, що задовольняють вимоги до безпеки, масштабованості та ефективності, водночас зберігаючи контроль над критично важливими даними та ресурсами. Для ефективної реалізації моделі інтеграції AWS і Eucalyptus необхідно забезпечити динамічну взаємодію між платформами, включаючи автоматизацію процесів і використання сучасних методів оркестрації. Одним із ключових підходів є впровадження інструментів для управління інфраструктурою як кодом (Infrastructure as Code), таких як Terraform або AWS CloudFormation. Ці інструменти дозволяють створювати уніфіковані конфігурації, які можна використовувати як у приватній хмарі Eucalyptus, так і в публічній хмарі AWS. Завдяки цьому розгортання інфраструктури стає більш швидким і прозорим, що знижує ризики помилок і забезпечує узгодженість конфігурацій на обох платформах.

Ще одним важливим аспектом є оптимізація використання ресурсів. Завдяки інтеграції AWS і Eucalyptus організації можуть краще управляти своїми ресурсами, розподіляючи навантаження між приватними і публічними хмарами залежно від

поточних потреб. Наприклад, обчислювальні завдання, які вимагають низької затримки, можуть виконуватися локально в Eucalyptus, тоді як завдання, що вимагають масштабування, можуть бути передані в AWS. Це дозволяє мінімізувати витрати, зберігаючи при цьому високу продуктивність системи.

Крім того, інтеграція підтримує реалізацію моделей розподілу робочих навантажень. Наприклад, у сценаріях, де організація працює в різних регіонах, Eucalyptus може обслуговувати локальні потреби, тоді як AWS може забезпечувати глобальну доступність ресурсів. Це особливо важливо для компаній, які працюють у міжнародних масштабах і потребують вирішення питань регіональної відповідності даних або зниження затримки для користувачів у різних куточках світу. Моніторинг і управління також є важливими компонентами інтеграційної моделі. Інструменти для моніторингу, такі як Amazon CloudWatch і Eucalyptus CloudWatch, дозволяють стежити за станом системи в реальному часі, забезпечуючи оперативну інформацію про продуктивність, використання ресурсів і потенційні проблеми. Завдяки цьому адміністратори можуть швидко реагувати на збої або аномалії, забезпечуючи стабільність і ефективність роботи системи.

Безпека в інтегрованій моделі відіграє ключову роль. Використання уніфікованих політик безпеки, які працюють як у приватній, так і в публічній хмарах, дозволяє захистити конфіденційні дані та уникнути порушень. Наприклад, шифрування даних під час передачі та зберігання забезпечує їхню захищеність незалежно від того, де вони знаходяться — у приватній чи публічній хмарі. Багаторівневі системи аутентифікації та управління доступом також допомагають мінімізувати ризики несанкціонованого доступу. На рисунку 3.2 відображені всі аспекти інтеграції AWS та Eucalyptus.

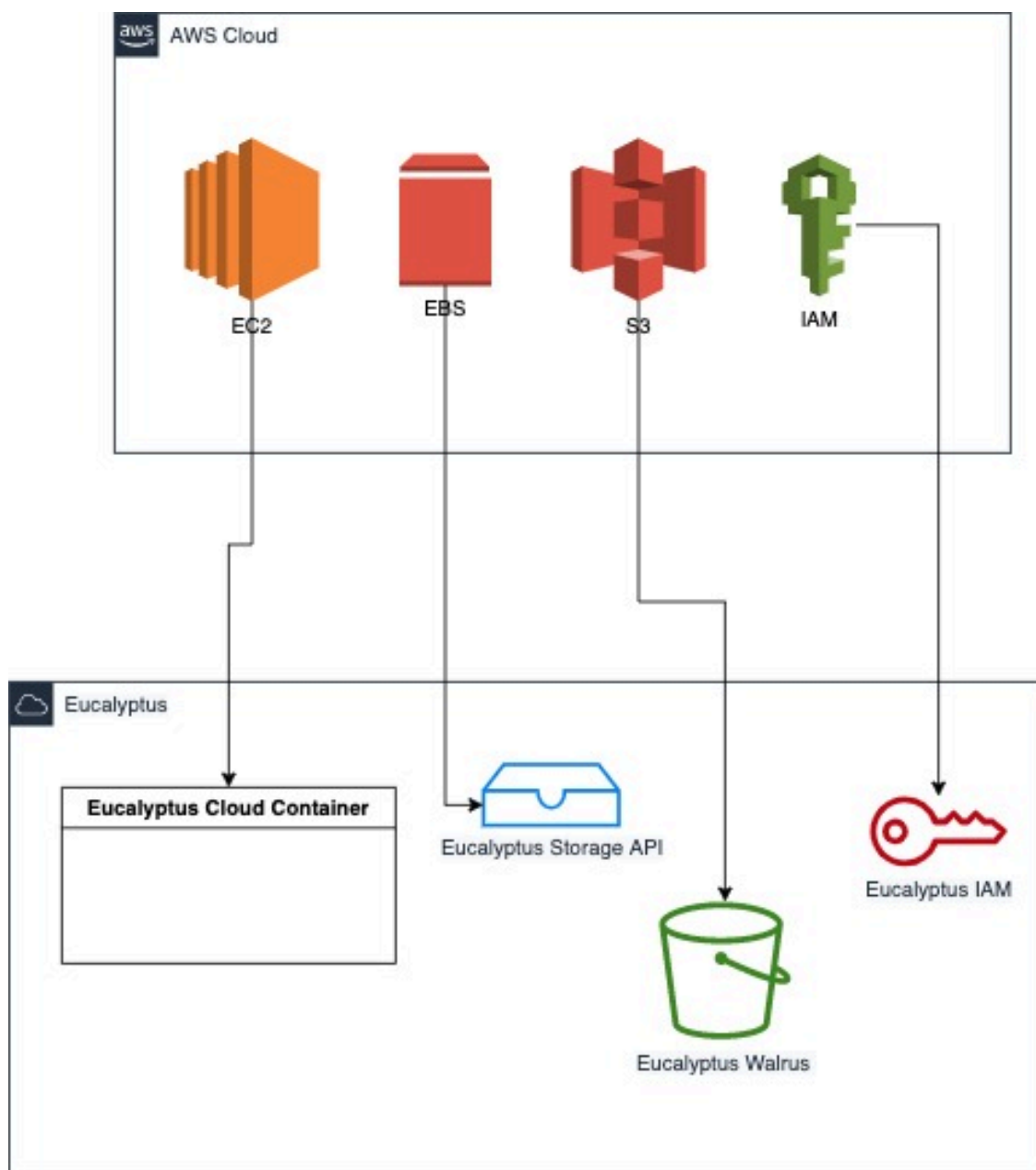


Рисунок 3.2 – Діаграма інтеграції

Для підвищення ефективності роботи інтегрованої системи також важливо врахувати питання відновлення після збоїв. Створення стратегій аварійного відновлення з використанням можливостей обох платформ дозволяє організаціям швидко відновлювати доступ до даних і ресурсів у разі збоїв. Наприклад, резервні копії, створені в приватній хмарі Eucalyptus, можуть бути автоматично перенесені в AWS, забезпечуючи додатковий рівень захисту даних.

Модель інтеграції також відкриває можливості для інновацій та розвитку. Поєднання можливостей приватних хмар Eucalyptus із широким спектром сервісів

AWS, таких як машинне навчання, аналітика даних або сервіси IoT, дозволяє організаціям впроваджувати нові технології без значних змін у їхній поточній інфраструктурі. Це забезпечує гнучкість і конкурентні переваги на ринку.

Модель інтеграції AWS і Eucalyptus забезпечує високий рівень гнучкості, масштабованості та безпеки, дозволяючи організаціям ефективно використовувати ресурси та адаптуватися до змінних потреб бізнесу. Вона є потужним інструментом для створення сучасних IT-рішень, які відповідають найвищим стандартам продуктивності та надійності.

```
import boto3
from botocore.exceptions import NoCredentialsError, PartialCredentialsError
# AWS Configuration
aws_access_key = "YOUR_AWS_ACCESS_KEY"
aws_secret_key = "YOUR_AWS_SECRET_KEY"
aws_region = "us-west-2"
# Eucalyptus Configuration
euca_endpoint = "https://your-eucalyptus-endpoint.com"
euca_access_key = "YOUR_EUCALYPTUS_ACCESS_KEY"
euca_secret_key = "YOUR_EUCALYPTUS_SECRET_KEY"
# Connect to AWS
try:
    aws_session = boto3.session.Session(
        aws_access_key_id=aws_access_key,
        aws_secret_access_key=aws_secret_key,
        region_name=aws_region
    )
    aws_ec2 = aws_session.client('ec2')
    aws_s3 = aws_session.client('s3')
    print("Successfully connected to AWS!")
except (NoCredentialsError, PartialCredentialsError) as e:
    print(f"Failed to connect to AWS: {e}")

# Connect to Eucalyptus
try:
```



```

euca_session = boto3.session.Session(
    aws_access_key_id=euca_access_key,
    aws_secret_access_key=euca_secret_key,
    region_name="eucalyptus",
    endpoint_url=euca_endpoint
)
euca_ec2 = euca_session.client('ec2')
euca_s3 = euca_session.client('s3')
print("Successfully connected to Eucalyptus!")
except (NoCredentialsError, PartialCredentialsError) as e:
    print(f"Failed to connect to Eucalyptus: {e}")

# Example AWS Operation: Launch an EC2 Instance
try:
    aws_ec2.run_instances(
        ImageId='ami-0abcdef1234567890',
        InstanceType='t2.micro',
        MinCount=1,
        MaxCount=1,
        KeyName='your-key-name'
    )
    print("AWS EC2 instance launched successfully!")
except Exception as e:
    print(f"Error launching AWS EC2 instance: {e}")

# Example Eucalyptus Operation: Create a Bucket in S3
try:
    euca_s3.create_bucket(Bucket='eucalyptus-bucket-example')
    print("Bucket created successfully in Eucalyptus!")
except Exception as e:
    print(f"Error creating bucket in Eucalyptus: {e}")

# Example Data Sync: Upload file to both AWS and Eucalyptus S3
file_path = "path/to/your/file.txt"
bucket_name = "your-bucket-name"

```

try:

Upload to AWS S3

aws_s3.upload_file(file_path, bucket_name, "file-in-aws.txt")

print("File uploaded to AWS S3!")

Upload to Eucalyptus S3

euca_s3.upload_file(file_path, bucket_name, "file-in-eucalyptus.txt")

print("File uploaded to Eucalyptus S3!")

except Exception as e:

print(f"Error uploading files: {e}")

Конфігурація: Замініть *YOUR_AWS_ACCESS_KEY*, *YOUR_AWS_SECRET_KEY*, *YOUR_EUCALYPTUS_ACCESS_KEY*, *YOUR_EUCALYPTUS_SECRET_KEY*, *ami-0abcdef1234567890*, та інші параметри на відповідні для вашої системи.

Інтеграція: Код використовує сумісність API між AWS та Eucalyptus для виконання схожих операцій, таких як створення екземплярів або завантаження даних у сховище S3.

Переконайтесь, що Boto3 встановлений (`pip install boto3`) і ваші ключі доступу мають необхідні права доступу.

4 АНАЛІЗ ЕФЕКТИВНОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІНТЕГРАЦІЇ ХМАРНИХ ПЛАТФОРМ

4.1 Показники ефективності інтеграції

Ключові показники ефективності, що використовуються для оцінки інтеграції хмарних платформ, дозволяють об'єктивно виміряти продуктивність, стабільність і якість взаємодії між різними системами. Вони є основою для аналізу ефективності рішень, ухвалених під час інтеграції, а також визначення шляхів подальшого вдосконалення. Ці показники не лише оцінюють технічні аспекти, але й дають змогу зрозуміти, як інтеграція впливає на бізнес-процеси та кінцевий користувацький досвід.

Швидкість обробки запитів є одним із найважливіших показників, оскільки вона визначає, наскільки оперативно система може виконувати завдання, які надходять від користувачів або інших систем. Для інтегрованих хмарних платформ швидкість обробки запитів є критичною, особливо якщо мова йде про сценарії з високим навантаженням, такі як обробка великих обсягів даних у реальному часі або виконання запитів, пов'язаних із транзакціями. Цей показник впливає на загальну продуктивність системи, адже затримки або повільна обробка можуть призводити до зниження ефективності роботи всіх компонентів.

Масштабованість також відіграє ключову роль у визначенні ефективності інтеграції. Цей показник оцінює здатність системи збільшувати або зменшувати обсяги ресурсів відповідно до поточних потреб. У контексті інтеграції хмарних платформ масштабованість дозволяє системі адаптуватися до змін у робочому навантаженні, наприклад, у пікові періоди або під час обробки великих обсягів даних. Висока масштабованість сприяє економії ресурсів, оскільки організації можуть уникати перевитрат на надлишкову інфраструктуру та водночас гарантувати стабільність роботи навіть за підвищеного навантаження.

Затримка доступу до ресурсів є ще одним важливим показником, який оцінює час, необхідний для виконання запиту від користувача або іншої системи до моменту отримання відповіді. Для інтеграції хмарних платформ цей показник є

особливо актуальним, оскільки затримка може виникати через складність маршрутизації, використання декількох хмарних середовищ або географічне розташування ресурсів. Мінімізація затримки є критично важливою для забезпечення швидкого доступу до даних, особливо в системах, які обслуговують користувачів у різних регіонах або працюють у режимі реального часу.

Стабільність роботи інтегрованих платформ оцінюється через показники, такі як час безвідмовної роботи (uptime) і середній час відновлення після збою (MTTR). Висока стабільність системи є результатом правильної інтеграції, яка забезпечує узгодженість між компонентами, резервування ресурсів і готовність до обробки збоїв. Наприклад, у випадку з інтегрованими платформами AWS і Eucalyptus стабільність визначає, наскільки добре обидві системи синхронізуються та взаємодіють без втрати даних або переривань у роботі. Економічна ефективність також може бути одним із показників, який оцінює, наскільки інтеграція дозволяє оптимізувати використання ресурсів і зменшити витрати. Цей показник охоплює не лише прямі витрати на інфраструктуру, але й непрямі фактори, такі як економія часу завдяки автоматизації процесів або зниження витрат на підтримку системи.

Інтеграція хмарних платформ також оцінюється через показники безпеки. Наприклад, кількість успішних атак або витоків даних може бути індикатором того, наскільки ефективно реалізована система безпеки в інтегрованому середовищі. Це особливо важливо для платформ, які обробляють конфіденційну інформацію або працюють у регульованих галузях. Окрім основних показників ефективності, таких як швидкість обробки запитів, масштабованість, затримка доступу, стабільність роботи, та економічна ефективність, важливо враховувати ще кілька додаткових метрик, які допомагають оцінити інтеграцію хмарних платформ у більш широкому контексті.

Один із таких показників — гнучкість інтеграції, що відображає здатність системи легко адаптуватися до змін у вимогах бізнесу або технологічному середовищі. Наприклад, якщо одна з платформ оновлює свої API чи додає нові сервіси, інтегрована система повинна підтримувати цю зміну без значних переробок. Гнучкість також включає здатність швидко розширювати

функціональність, додаючи нові сервіси або інтегруючи додаткові платформи. Це стає критично важливим для організацій, які працюють у динамічних галузях, де інновації є ключовим фактором успіху.

Продуктивність даних є ще одним важливим показником, який визначає, наскільки ефективно система інтеграції обробляє великі обсяги інформації. Ця метрика враховує швидкість передачі даних між платформами, час обробки запитів до баз даних, а також здатність до аналітики в реальному часі. Інтеграція AWS та Eucalyptus, наприклад, може покращувати продуктивність даних завдяки поєднанню локальних сховищ з високою швидкістю доступу та потужних аналітичних інструментів AWS.

Сумісність між платформами є показником, який визначає, наскільки добре різні компоненти інтегрованої системи можуть взаємодіяти між собою. Це включає не тільки технічну сумісність (наприклад, відповідність API або протоколів передачі даних), але й узгодженість у підходах до безпеки, управління доступом і моніторингу. Висока сумісність забезпечує безшовний обмін інформацією та знижує ризики втрати даних або несумісності між системами.

Важливим аспектом є користувацький досвід (UX), який відображає, наскільки зручно користувачам працювати з інтегрованими платформами. Наприклад, якщо доступ до обчислювальних ресурсів або даних займає надто багато часу, це може вплинути на ефективність роботи користувачів і створити негативне враження про систему. Інтеграція повинна спрощувати роботу користувачів, автоматизуючи рутинні завдання, забезпечуючи швидкий доступ до даних і ресурсів, а також пропонуючи зручні інтерфейси для управління.

Екологічна ефективність — показник, що стає все більш актуальним у сучасному світі. Він оцінює, наскільки енергоефективно працює інтегрована система, враховуючи споживання енергії як у локальних, так і в публічних хмарах. Зниження енергоспоживання не тільки зменшує витрати, але й сприяє виконанню корпоративних цілей сталого розвитку, що є важливим для репутації компанії.

Також варто враховувати операційну прозорість, яка визначає, наскільки легко адміністратори можуть відслідковувати та аналізувати стан інтегрованої

системи. Це включає доступ до метрик продуктивності, логів системи, а також сповіщення про потенційні проблеми. Прозорість допомагає запобігати збої та швидко реагувати на них, що підвищує загальну ефективність системи.

Отже, комплексний підхід до оцінки інтеграції хмарних платформ включає як базові технічні показники, так і додаткові метрики, які відображають адаптивність, взаємодію між компонентами, зручність для користувачів, екологічну ефективність і прозорість управління. Аналіз цих показників дозволяє забезпечити збалансований розвиток інтегрованої інфраструктури, яка задовольняє поточні та майбутні потреби організації. Інтеграція хмарних платформ значно впливає на загальні витрати організації, оскільки забезпечує нові можливості для оптимізації як операційних витрат, так і капіталовкладень в інфраструктуру. Завдяки використанню хмарних платформ організації можуть адаптувати свої витрати до реальних потреб, знижуючи навантаження на бюджет і підвищуючи ефективність використання ресурсів.

Однією з головних переваг інтеграції є зниження капітальних витрат. Замість того, щоб інвестувати значні кошти у створення та підтримку власної інфраструктури, організації можуть орендувати необхідні обчислювальні ресурси у хмарних провайдерів. Наприклад, інтеграція приватної хмари Eucalyptus із публічною хмарою AWS дозволяє зберігати критично важливі дані та програми локально, тоді як додаткові ресурси, необхідні для обробки пікових навантажень, можуть бути залучені з публічної хмари. Це знижує потребу у дорогому обладнанні та його обслуговуванні.

Операційні витрати також зменшуються завдяки гнучкості хмарних платформ. Більшість хмарних провайдерів пропонують моделі оплати на основі використання (pay-as-you-go), що дозволяє організаціям оплачувати лише ті ресурси, які фактично використовуються. Це особливо корисно для компаній із нерівномірним навантаженням на ІТ-інфраструктуру, наприклад, у періоди пікової активності. Інтеграція дозволяє автоматично масштабувати ресурси, забезпечуючи ефективне використання потужностей без переплати за надлишкові ресурси.

Крім того, інтеграція сприяє оптимізації витрат на підтримку та управління інфраструктурою. Використання хмарних платформ дозволяє автоматизувати багато рутинних завдань, таких як резервне копіювання, оновлення програмного забезпечення або моніторинг систем. Наприклад, сервіси AWS, такі як CloudWatch для моніторингу або Backup для створення резервних копій, зменшують потребу у великій кількості ІТ-персоналу для виконання цих функцій. Це не лише знижує витрати, але й підвищує ефективність роботи команди, дозволяючи їй зосередитися на більш стратегічних завданнях.

Інтеграція хмарних платформ також допомагає знизити витрати, пов'язані зі збоєм у роботі або втратами даних. Завдяки механізмам аварійного відновлення (disaster recovery) та високій доступності хмарних ресурсів, організації можуть мінімізувати час простою та уникнути значних фінансових втрат. Наприклад, у разі відмови локальної інфраструктури Eucalyptus, резервні копії даних можуть бути швидко завантажені з AWS, забезпечуючи безперервність бізнес-процесів.

Ще одним важливим аспектом є економія на енергоспоживанні. Локальна інфраструктура часто потребує значних витрат на електроенергію для живлення серверів та їх охолодження. Використання хмарних ресурсів дозволяє зменшити ці витрати, оскільки енергоспоживання переноситься на провайдера хмарних послуг, який, як правило, має більш енергоефективні дата-центри. Окрім безпосередніх фінансових вигод, інтеграція сприяє стратегічній оптимізації витрат. Організації можуть уникати надлишкових інвестицій у інфраструктуру, яка може стати застарілою або не відповідати вимогам бізнесу в майбутньому. Замість цього вони отримують доступ до новітніх технологій і можуть швидко адаптуватися до змін у ринкових умовах або вимогах клієнтів. Інтеграція хмарних платформ створює економічні переваги завдяки гнучкості використання ресурсів, зниженню капітальних та операційних витрат, оптимізації управління інфраструктурою, підвищенню стійкості до збоїв і зниженню енергоспоживання. Ці переваги роблять хмарну інтеграцію ефективним рішенням для організацій, які прагнуть підвищити свою конкурентоспроможність і зменшити фінансові ризики.

Ре Інтеграція хмарних платформ має значний вплив на безпеку даних та відповідність стандартам, оскільки вона об'єднує різні інфраструктури, технології та системи управління, створюючи нові можливості та виклики для забезпечення безпеки. Інтеграція може підвищити рівень захисту даних через використання передових технологій безпеки та забезпечення узгодженості між різними платформами, але при цьому вимагає ретельного управління ризиками.

Одним із ключових аспектів впливу є підвищення рівня захищеності передачі даних. Інтеграція дозволяє використовувати шифрування на всіх етапах передачі інформації між платформами, забезпечуючи захист даних від перехоплення або несанкціонованого доступу. Наприклад, при інтеграції приватної хмари Eucalyptus із публічною хмарою AWS можуть бути використані такі протоколи, як TLS (Transport Layer Security), які гарантують безпечну передачу даних навіть через відкриті мережі. Це особливо важливо для організацій, які працюють з конфіденційною інформацією, такою як фінансові дані чи медичні записи.

Відповідність стандартам і регуляторним вимогам є ще одним важливим аспектом, який впливає на інтеграцію. Організації, що працюють у регульованих галузях, повинні дотримуватися таких стандартів, як GDPR (General Data Protection Regulation) або HIPAA (Health Insurance Portability and Accountability Act). Інтеграція хмарних платформ може забезпечити централізоване управління політиками безпеки, що дозволяє дотримуватись цих вимог. Наприклад, AWS пропонує інструменти для створення політик відповідності, які дозволяють автоматично перевіряти дотримання стандартів у реальному часі. Однак інтеграція також створює нові ризики, такі як складність управління доступом до даних у різних середовищах. Для їхнього вирішення використовуються сучасні системи управління доступом, наприклад AWS IAM (Identity and Access Management), які дозволяють визначати детальні політики доступу до ресурсів. Ці системи можуть бути інтегровані з локальними рішеннями в приватній хмарі, забезпечуючи єдину точку управління доступом. Це значно знижує ризик несанкціонованого доступу, який може виникнути через помилки в налаштуваннях або людський фактор.

Для оцінки впливу інтеграції на безпеку даних використовуються різні показники. Одним із найважливіших є кількість інцидентів безпеки, таких як зломи, витоки даних або несанкціонований доступ. Цей показник дозволяє оцінити, наскільки добре система захищена після інтеграції. Зменшення кількості інцидентів свідчить про ефективність впроваджених заходів безпеки.

Ще одним показником є рівень відповідності політик безпеки регуляторним вимогам. Наприклад, організація може регулярно проводити аудити відповідності та аналізувати, наскільки інтегрована система відповідає стандартам, що застосовуються у галузі. Відсутність порушень або санкцій з боку регулюючих органів є індикатором успішної інтеграції [18].

Інтеграція також впливає на рівень прозорості управління безпекою. Це може бути оцінено через наявність централізованих інструментів моніторингу та управління, які дозволяють адміністраторам в реальному часі відстежувати стан безпеки системи. Наприклад, сервіси AWS CloudTrail та Eucalyptus CloudWatch забезпечують журналювання всіх операцій у хмарі, що допомагає швидко виявляти та реагувати на загрози. Рівень захищеності передачі даних оцінюється через метрики, такі як кількість зашифрованих транзакцій, частота використання протоколів шифрування та час реагування на можливі атаки. Ці показники дозволяють визначити, наскільки інтегрована система захищає дані під час їхньої передачі. Інтеграція хмарних платформ може значно покращити безпеку даних та забезпечити відповідність стандартам, але для цього необхідно впроваджувати сучасні технології захисту, централізовані системи управління доступом і механізми моніторингу. Аналіз показників, таких як кількість інцидентів, рівень відповідності стандартам і захищеність передачі даних, дозволяє оцінити ефективність інтеграції та забезпечити високий рівень безпеки у всій системі. Методи вимірювання стабільності та доступності інтегрованих систем мають ключове значення для забезпечення високої якості користувацького досвіду, оскільки вони дозволяють виявляти та усувати проблеми, що впливають на роботу системи. Основними показниками для оцінки стабільності є час безвідмовної роботи (uptime), середній час відновлення після збою (MTTR) та затримка доступу

до даних. Ці метрики є індикаторами того, наскільки надійною і швидкою є система для кінцевих користувачів.

Час безвідмовної роботи (uptime) вимірює відсоток часу, протягом якого система доступна для користувачів і працює без збоїв. Цей показник є критичним для оцінки стабільності, особливо для хмарних платформ, що забезпечують постійний доступ до даних і сервісів. Для його вимірювання використовуються автоматизовані системи моніторингу, такі як AWS CloudWatch або Zabbix, які у реальному часі відстежують стан системи та сповіщають про будь-які збої. Високий uptime (наприклад, 99.99%) означає, що користувачі рідко стикаються з недоступністю сервісів, що суттєво покращує їхній досвід.

Середній час відновлення після збою (MTTR) оцінює, скільки часу потрібно для відновлення системи після виникнення проблеми. Цей показник є особливо важливим для інтегрованих систем, де будь-яка затримка у відновленні може вплинути на роботу бізнесу або завдати значних фінансових збитків. Для зменшення MTTR застосовуються інструменти для автоматизації процесів відновлення, такі як резервне копіювання, автоматичне перемикавання на резервні системи (failover) або оркестрація відновлення. Наприклад, у разі збою у приватній хмарі Eucalyptus система може автоматично переключитися на ресурси AWS, що мінімізує час простою. Затримка доступу до даних є ще одним важливим показником, який вимірює час, необхідний для виконання запиту користувача до моменту отримання відповіді. Висока затримка може створювати негативний досвід для користувачів, особливо якщо вони працюють із реальним часом або великими обсягами даних. Для вимірювання затримки використовуються інструменти тестування продуктивності, такі як Apache JMeter або Pingdom, які дозволяють відстежувати час відгуку системи на запити з різних географічних регіонів. Зменшення затримки досягається за допомогою оптимізації мережевої інфраструктури, використання кешування та розподілених систем зберігання даних.

Метрики стабільності також включають кількість збоїв за певний період часу, середню тривалість простоїв та частоту аварійних ситуацій. Ці показники

допомагають зрозуміти, наскільки часто система стикається з проблемами, і дозволяють розробникам вживати заходів для їхнього зменшення. Наприклад, інтеграція систем резервування, регулярне оновлення програмного забезпечення та моніторинг вразливостей можуть значно знизити кількість збоїв. Стабільність і доступність інтегрованих систем безпосередньо впливають на користувацький досвід. Якщо система працює стабільно і забезпечує швидкий доступ до даних, користувачі сприймають її як надійну та ефективну. Висока доступність також підвищує довіру до організації, яка надає ці сервіси. З іншого боку, часті збої, тривалий час відновлення або затримка доступу можуть викликати невдоволення користувачів, знизити їхню продуктивність та навіть призвести до втрати клієнтів.

Отже, вимірювання стабільності та доступності інтегрованих систем за допомогою таких показників, як uptime, MTTR і затримка доступу, дозволяє забезпечити високий рівень обслуговування та мінімізувати вплив проблем на користувачів. Ці метрики є основою для покращення якості роботи системи, зменшення ризиків та підвищення задоволеності користувачів.

4.2 Вплив інтеграції на продуктивність мережевої інфраструктури

Інтеграція хмарних платформ значно впливає на продуктивність мережевої інфраструктури, забезпечуючи гнучкість, масштабованість і оптимізацію роботи системи. Цей вплив проявляється у кількох ключових аспектах, які мають вирішальне значення для сучасних організацій, що використовують хмарні технології.

По-перше, інтеграція дозволяє оптимізувати використання обчислювальних і мережевих ресурсів. Завдяки можливості динамічного розподілу навантаження між приватними і публічними хмарами, організації можуть уникнути перевантаження локальних мережевих компонентів. Наприклад, у разі пікового навантаження частина обчислень або зберігання даних може бути перенесена з приватної хмари Eucalyptus до публічної платформи AWS, що дозволяє зберегти стабільність роботи інфраструктури без зниження продуктивності. Ця гнучкість

також дозволяє ефективно управляти пропускнуою здатністю мережі, знижуючи затримки та покращуючи загальну продуктивність.

По-друге, інтеграція покращує продуктивність завдяки використанню сучасних технологій балансування навантаження. Вбудовані інструменти, такі як Elastic Load Balancing (ELB) в AWS, забезпечують рівномірний розподіл трафіку між кількома вузлами мережі, що запобігає перевантаженням і збої в роботі системи. Це особливо важливо для інтегрованих платформ, які обробляють великі обсяги даних або обслуговують значну кількість користувачів одночасно. Завдяки балансуванню навантаження підвищується ефективність використання мережевих ресурсів, що сприяє швидшій обробці запитів і покращує користувацький досвід.

По-третє, інтеграція сприяє зменшенню затримок у передачі даних. Використання розподілених центрів обробки даних дозволяє забезпечити близькість обчислювальних ресурсів до кінцевих користувачів. Наприклад, AWS має мережу глобальних дата-центрів, які можуть бути інтегровані з локальними ресурсами Eucalyptus для створення гібридної інфраструктури. Це зменшує час доступу до даних і сервісів, оскільки запити обробляються у найближчому доступному вузлі. Зменшення затримок є критично важливим для додатків, які працюють у реальному часі, таких як онлайн-трансляції або фінансові сервіси.

По-четверте, інтеграція дозволяє підвищити ефективність управління мережевою інфраструктурою. Завдяки централізованим інструментам моніторингу, таким як Amazon CloudWatch або Eucalyptus CloudWatch, адміністратори можуть в реальному часі відстежувати стан мережі, аналізувати продуктивність і виявляти потенційні проблеми до того, як вони вплинуть на роботу системи. Це дозволяє швидко реагувати на зміни в навантаженні або усувати несправності, що забезпечує стабільну роботу інфраструктури.

По-п'яте, інтеграція створює можливості для автоматизації процесів, які впливають на продуктивність мережі. Наприклад, автоматичне масштабування обчислювальних потужностей у AWS дозволяє динамічно додавати чи видаляти ресурси залежно від поточних потреб. Це знижує ризик перевантаження мережі і

забезпечує стабільну продуктивність навіть у періоди високої активності користувачів.

Нарешті, інтеграція сприяє покращенню безпеки мережі, що також позитивно впливає на її продуктивність. Завдяки використанню сучасних протоколів шифрування та систем управління доступом, таких як AWS IAM, інтегровані платформи можуть захистити дані під час передачі та запобігти загрозам, які можуть порушити роботу мережі. Високий рівень безпеки дозволяє уникнути простоїв і забезпечити надійну роботу всієї інфраструктури.

Отже, інтеграція хмарних платформ істотно підвищує продуктивність мережевої інфраструктури, покращуючи управління ресурсами, зменшуючи затримки, забезпечуючи стабільність і безпеку. Ці переваги роблять інтеграцію ефективним інструментом для організацій, які прагнуть підвищити ефективність своєї мережі та забезпечити високий рівень обслуговування користувачів. Додатковим аспектом впливу інтеграції на продуктивність мережевої інфраструктури є здатність масштабувати обчислювальні ресурси в залежності від поточних потреб бізнесу. Ця властивість дозволяє організаціям гнучко адаптувати інфраструктуру до змін у робочому навантаженні, що особливо важливо для сучасних компаній, які працюють у динамічних ринкових умовах. Наприклад, інтеграція приватної хмари Eucalyptus з публічною платформою AWS дає змогу автоматично переміщувати ресурси між двома середовищами, що забезпечує безперервну роботу навіть у періоди пікової активності.

Ще однією перевагою є використання механізмів оптимізації трафіку, які забезпечують ефективний обмін даними між різними вузлами мережі. Наприклад, хмарні платформи дозволяють застосовувати інтелектуальні алгоритми маршрутизації трафіку, які враховують навантаження на канали зв'язку, географічне розташування користувачів та пріоритетність запитів. Це дозволяє зменшити затримки в обробці даних та підвищити загальну швидкість роботи системи. Крім того, інтеграція створює умови для покращення надійності мережі через впровадження систем резервування та відновлення. Завдяки можливостям гібридної архітектури, організації можуть створювати резервні копії даних і

сервісів у публічній хмарі, забезпечуючи швидке відновлення у разі збоїв у локальній інфраструктурі. Наприклад, у разі несправності серверів у приватній хмарі, інтеграція з AWS дозволяє перенаправляти трафік до резервних вузлів, мінімізуючи час простою і втрату даних.

Інтеграція також сприяє вдосконаленню механізмів обробки великих обсягів даних. Сучасні хмарні платформи пропонують інструменти для аналізу великих даних у реальному часі, які можуть бути інтегровані у мережеву інфраструктуру. Це дозволяє організаціям обробляти та аналізувати дані швидше та ефективніше, що особливо важливо для бізнесів, які працюють з потоковими даними або великими обсягами структурованої інформації.

Значним фактором є і зменшення адміністративного навантаження на ІТ-відділи. Інтегровані хмарні платформи надають централізовані панелі управління та автоматизовані системи моніторингу, які значно спрощують адміністрування мережевої інфраструктури. Це дозволяє ІТ-фахівцям зосередитися на стратегічних завданнях, таких як оптимізація продуктивності або впровадження нових технологій, замість вирішення рутинних проблем. Крім технічних переваг, інтеграція також впливає на користувацький досвід. Завдяки підвищеній швидкості доступу до даних, зниженню затримок та стабільності роботи системи користувачі отримують більш якісний сервіс. Це особливо важливо для бізнесів, які працюють у сфері електронної комерції, фінансових послуг або медіа, де затримки у доступі до ресурсів можуть негативно вплинути на рівень задоволеності клієнтів. Більш детально вплив інтеграції відображено в таблиці 4.1.

Таблиця 4.1 Вплив інтеграції на продуктивність мережевої інфраструктури

Аспект продуктивності	Опис впливу інтеграції
Гнучкість і масштабованість	Інтеграція дозволяє динамічно розподіляти ресурси між приватними та публічними хмарами залежно від навантаження, забезпечуючи стабільність і ефективність роботи.

Продовження таблиці 4.1 Вплив інтеграції на продуктивність мережевої інфраструктури

Оптимізація трафіку	Використання інтелектуальних алгоритмів маршрутизації трафіку зменшує затримки передачі даних і підвищує швидкість доступу до ресурсів.
Надійність мережі	Системи резервування та аварійного відновлення забезпечують мінімізацію часу простою і втрат даних у разі збоїв у мережі.
Обробка великих даних	Інструменти для аналізу великих даних у реальному часі дозволяють швидко обробляти потоки інформації, що підвищує ефективність бізнес-процесів.
Зниження адміністративного навантаження	Централізовані панелі управління та автоматизовані системи моніторингу знижують навантаження на ІТ-персонал, спрощуючи адміністрування.
Покращення користувацького досвіду	Завдяки високій швидкості доступу, стабільності роботи і низьким затримкам користувачі отримують якісний і швидкий сервіс.

Інтеграція хмарних платформ є потужним інструментом для покращення продуктивності мережевої інфраструктури. Вона забезпечує ефективне використання ресурсів, оптимізацію трафіку, підвищення надійності та вдосконалення механізмів обробки даних, водночас покращуючи користувацький досвід і знижуючи адміністративні витрати. Ці переваги дозволяють організаціям залишатися конкурентоспроможними, впроваджуючи новітні технології та адаптуючись до змін у бізнес-середовищі.

4.3 Перспективи використання гібридних хмарних середовищ

Перспективи використання гібридних хмарних середовищ є надзвичайно значущими для сучасних організацій, оскільки вони поєднують переваги приватних і публічних хмар, дозволяючи досягти високої гнучкості, масштабованості, економічної ефективності та безпеки. Гібридна архітектура забезпечує можливість адаптувати ІТ-інфраструктуру до специфічних вимог бізнесу, що робить її особливо привабливою для організацій, які прагнуть впроваджувати інновації та залишатися конкурентоспроможними.

Однією з ключових перспектив є гнучке управління робочими навантаженнями. Гібридні хмарні середовища дозволяють розподіляти навантаження між приватними і публічними хмарами залежно від поточних потреб. Наприклад, критично важливі дані та програми можуть зберігатися у приватній хмарі, де забезпечується високий рівень контролю і безпеки, тоді як ресурсоемні задачі, які потребують масштабування, можуть виконуватися у публічній хмарі. Це дозволяє оптимально використовувати ресурси і знижувати витрати.

Ще однією важливою перспективою є підвищення надійності і стійкості до збоїв. Гібридна архітектура забезпечує можливість створення резервних копій даних у різних середовищах, що дозволяє швидко відновлювати роботу системи у разі збоїв або кібератак. Наприклад, у разі виходу з ладу приватної хмари, дані можуть бути автоматично відновлені з публічної хмари, що мінімізує час простою і втрату інформації. Такий підхід особливо корисний для організацій, які працюють з критично важливими додатками, де перерви у роботі можуть призвести до значних фінансових або репутаційних збитків.

Гібридні хмарні середовища також відкривають широкі можливості для інновацій. Вони забезпечують доступ до передових технологій, які пропонують провайдери публічних хмар, таких як машинне навчання, штучний інтелект або інструменти аналізу великих даних. Це дозволяє організаціям впроваджувати нові підходи до обробки інформації і створення цінності для клієнтів, не вкладаючи значні кошти у розвиток власної інфраструктури. Наприклад, підприємство може

використовувати хмарні сервіси для аналізу клієнтської поведінки у реальному часі, щоб пропонувати персоналізовані рішення.

Крім того, гібридна архітектура сприяє підвищенню безпеки даних і відповідності стандартам. Організації можуть зберігати конфіденційну інформацію у приватній хмарі, дотримуючись локальних регуляторних вимог, таких як GDPR або HIPAA, і водночас використовувати публічну хмару для зберігання менш критичних даних. Такий підхід дозволяє забезпечити баланс між гнучкістю і дотриманням нормативних вимог, що є критично важливим для компаній у регульованих галузях, таких як фінанси або охорона здоров'я.

Економічна ефективність також є значною перевагою гібридних хмар. Організації можуть оптимізувати витрати, оплачуючи лише ті ресурси, які вони фактично використовують у публічній хмарі, і уникаючи значних капітальних вкладень у розвиток локальної інфраструктури. Це дозволяє знижувати загальні витрати на ІТ і водночас забезпечувати необхідний рівень продуктивності і масштабованості.

Нарешті, гібридні хмарні середовища сприяють покращенню користувацького досвіду. Завдяки зниженню затримок у доступі до даних і підвищенню стабільності роботи системи користувачі отримують швидкий і безперебійний доступ до сервісів. Це особливо важливо для глобальних компаній, які обслуговують клієнтів у різних регіонах і потребують забезпечення стабільної роботи своїх додатків у будь-який час.

Перспективи використання гібридних хмарних середовищ полягають у їхній здатності забезпечувати ефективне управління ресурсами, високу надійність, доступ до інновацій, підвищення безпеки і відповідності стандартам, а також зниження витрат. Вони є важливим інструментом для організацій, які прагнуть впроваджувати новітні технології і водночас забезпечувати стабільність і гнучкість своєї ІТ-інфраструктури. Крім того, перспективи гібридних хмарних середовищ включають їхню роль у підтримці бізнесу в умовах зростаючої складності ІТ-ландшафту. Сучасні компанії стикаються з постійно зростаючими вимогами до обробки даних, швидкості доступу та адаптації до ринкових змін. Гібридна хмарна

архітектура дозволяє вирішувати ці завдання, забезпечуючи високу гнучкість і адаптивність системи. Організації можуть створювати складні інфраструктури, які поєднують локальні ресурси, приватні хмари та публічні сервіси, щоб максимально ефективно використовувати доступні можливості.

Важливим фактором є здатність гібридних хмарних середовищ підтримувати безперервність бізнес-процесів у кризових ситуаціях. Нестабільність ринку, природні катастрофи або кібератаки можуть серйозно впливати на роботу організацій. Гібридна архітектура забезпечує резервування та географічне розподілення даних, що дозволяє зменшити ризики втрати інформації або збоїв у роботі системи. Завдяки цьому компанії можуть швидше відновлювати роботу та уникати серйозних фінансових чи репутаційних втрат.

Інша важлива перспектива пов'язана з інтеграцією хмарних технологій у бізнес-моделі майбутнього як показано в таблиці 4.2. Гібридні хмари стають основою для розробки концепцій, таких як цифрові близнюки, IoT-платформи, інтелектуальні мережі та розподілені системи обробки даних. Завдяки своїй здатності поєднувати обчислювальні ресурси з різних джерел, гібридна архітектура відкриває нові можливості для розвитку технологій, які покращують ефективність та інноваційність компаній. Гібридні хмари також відіграють значну роль у забезпеченні стійкості до змін у ринкових умовах. Наприклад, організації можуть швидко масштабувати свої ресурси для підтримки нових продуктів або сервісів, експериментувати з новими бізнес-моделями або адаптуватися до змін у споживчій поведінці. Така гнучкість дозволяє компаніям залишатися конкурентоспроможними навіть у швидко змінюваному середовищі. Крім того, перспективи гібридних хмар включають розширення можливостей автоматизації. Інтеграція сучасних інструментів управління хмарними ресурсами, таких як Kubernetes або Terraform, дозволяє автоматизувати процеси розгортання, масштабування та моніторингу. Це не лише знижує витрати, але й зменшує кількість помилок, пов'язаних із людським фактором, забезпечуючи більш стабільну роботу інфраструктури [19].

Таблиця 4.2 Перспективи використання гібридних хмарних середовищ

Переваги гібридних хмар	Опис перспектив
Гнучке управління навантаженнями	Забезпечення оптимального розподілу обчислювальних ресурсів між приватними та публічними хмарами залежно від потреб бізнесу.
Висока надійність і стійкість до збоїв	Створення резервних копій та відновлення даних у разі збоїв, мінімізуючи ризик простою.
Доступ до інноваційних технологій	Використання передових технологій, таких як штучний інтелект і машинне навчання, для підвищення ефективності процесів.
Підвищення безпеки даних	Зберігання конфіденційних даних у приватних хмарах з дотриманням регуляторних вимог і використання публічних хмар для менш критичних даних.
Економічна ефективність	Зниження витрат на ІТ-інфраструктуру за рахунок моделі оплати за використання та уникнення надлишкових інвестицій.
Покращення користувацького досвіду	Забезпечення стабільного і швидкого доступу до сервісів, зменшення затримок і підвищення рівня задоволеності клієнтів.
Підтримка безперервності бізнесу	Можливість швидкого відновлення роботи після кризових ситуацій завдяки резервуванню та географічному розподілу ресурсів.
Адаптивність до ринкових змін	Здатність швидко адаптувати ресурси до змін у вимогах ринку, впровадження нових бізнес-моделей.
Можливість розширення міжнародної присутності	Використання публічних хмар для надання послуг у віддалених регіонах без необхідності створення локальних дата-центрів.

Гібридні хмари також створюють умови для розширення міжнародної присутності організацій. Використовуючи публічні хмарні сервіси, компанії можуть надавати свої послуги у віддалених регіонах без необхідності будівництва локальних дата-центрів. Це дозволяє зменшити витрати на інфраструктуру та швидше виходити на нові ринки, задовольняючи потреби клієнтів незалежно від їхнього місця розташування. Загалом, перспективи використання гібридних хмарних середовищ підкреслюють їхню ключову роль у побудові стійких, інноваційних і економічно ефективних IT-інфраструктур. Вони дозволяють організаціям не лише вирішувати поточні завдання, але й готуватися до викликів майбутнього, забезпечуючи довгострокову конкурентоспроможність і стійкий розвиток.

ВИСНОВКИ

У висновках дипломної роботи підсумовано результати дослідження інтеграції хмарних платформ на прикладі AWS та Eucalyptus, а також їх вплив на продуктивність, ефективність та безпеку IT-інфраструктури. Було доведено, що гібридні хмарні середовища забезпечують унікальне поєднання масштабованості публічних хмар і контролю приватних платформ, що дозволяє вирішувати завдання сучасних організацій у динамічному бізнес-середовищі.

Одним із головних результатів є підтвердження значного підвищення гнучкості управління IT-ресурсами за рахунок інтеграції. Це дозволяє організаціям швидко адаптуватися до змін у навантаженні, розподіляти критично важливі завдання між приватними та публічними хмарами, а також знижувати витрати на інфраструктуру завдяки оптимізації ресурсів. Важливим аспектом стало впровадження сучасних інструментів для автоматизації управління, які мінімізують людський фактор та підвищують стабільність системи. Було встановлено, що інтеграція позитивно впливає на безпеку даних, дозволяючи організаціям поєднувати високий рівень захисту приватних хмар з додатковими можливостями публічних платформ. Використання сучасних протоколів шифрування, систем управління доступом і моніторингу забезпечує надійний захист інформації навіть у складній багатокомпонентній інфраструктурі.

Результати дослідження показали, що продуктивність мережевої інфраструктури значно покращується завдяки можливості балансування навантаження, зменшенню затримок передачі даних та інтеграції інструментів для аналізу великих обсягів інформації. Це дозволяє організаціям ефективніше виконувати свої бізнес-завдання, підвищуючи задоволеність клієнтів та конкурентоспроможність.

Окрему увагу приділено економічним аспектам інтеграції, що довело її високу рентабельність. Модель оплати за фактичне використання ресурсів, уникнення значних капітальних інвестицій у локальну інфраструктуру та

можливість швидкого масштабування забезпечують значне зниження витрат і підвищення економічної ефективності.

Дослідження також показало перспективи гібридних хмарних середовищ у контексті їхнього впливу на інновації, безперервність бізнес-процесів та адаптивність до змін. Ці платформи стають фундаментом для впровадження новітніх технологій, таких як штучний інтелект, IoT та аналітика великих даних, що відкриває нові можливості для розвитку організацій. У підсумку, результати дипломної роботи підтверджують доцільність і ефективність використання інтеграції хмарних платформ. Запропонована модель інтеграції забезпечує значне підвищення продуктивності, безпеки та економічної ефективності ІТ-інфраструктури, що робить її перспективним рішенням для широкого спектра сучасних бізнесів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Андрущенко, С. М. (2020). Хмарні обчислення як основа сучасних бізнес-рішень. *Бізнес та технології*, 14(3), 35-42.
2. Бондаренко, І. А. (2019). Хмарна безпека: основні виклики та шляхи вирішення. *Захист інформації в умовах сучасності*, 4(2), 10-17.
3. Бойко, І. М. (2020). Хмарні технології в управлінні IT-інфраструктурою підприємств. Київ: *Технології розвитку*.
4. Данилюк, М. С. (2021). Перспективи розвитку мультихмарних рішень у бізнесі. *Бізнес та інновації*, 14(6), 18-25.
5. Дуброва, Г. М. (2021). Інтеграція AWS та приватних хмар: практичні аспекти. *Хмарні технології в бізнесі*, 9(3), 23-29.
6. Зубарєв, П. Г. (2019). Тенденції розвитку хмарних технологій у корпоративному секторі. *Бізнес-аналітика*, 12(4), 38-45.
7. Іваненко, П. С. (2019). AWS та Eucalyptus: інтеграція хмарних платформ у бізнес-процеси. *Вісник інноваційних досліджень*, 8(4), 67-72.
8. Коваленко, О. В. (2021). Гібридні хмарні середовища: переваги та перспективи застосування. *Журнал сучасних технологій*, 12(3), 45-56.
9. Коцюбинський, О. Г. (2022). AWS Lambda та її застосування в автоматизації бізнес-процесів. *Практичний журнал хмарних технологій*, 7(4), 29-37.
10. Кравченко, Л. Д. (2020). Моделювання гібридних хмарних архітектур. *Інформаційні системи в управлінні*, 6(3), 20-28.
11. Кузьменко, О. С. (2022). Хмарні сервіси для аналізу великих даних: прикладні аспекти. *Інформаційні технології і моделі*, 11(5), 43-50.
12. Куліш, Ю. П. (2020). Контейнеризація додатків у гібридних хмарах. *Хмарні обчислення в практиці*, 9(2), 22-29.
13. Лазаренко, Н. І. (2021). Оркестрація контейнерів у хмарних платформах. *Хмарні обчислення: теорія і практика*, 5(7), 30-40.
14. Мельник, А. В. (2020). Економічна ефективність гібридних хмар. *Журнал економічних досліджень*, 19(4), 54-60.

15. Мороз, І. В. (2019). AWS EC2 та його роль у масштабуванні бізнес-процесів. *Хмарні платформи*, 13(4), 30-36.
16. Павленко, Н. І. (2021). Інструменти автоматизації в інтегрованих хмарних середовищах. *Хмарні обчислення: практика і досвід*, 5(6), 12-20.
17. Романенко, О. Д. (2022). Управління хмарною інфраструктурою на основі AWS та Eucalyptus. *Інформаційні системи і мережі*, 11(3), 20-28.
18. Смирнов, Ю. Л., & Гончарук, М. П. (2022). Безпека даних у гібридних хмарах: підходи та рішення. *Захист інформації*, 15(2), 24-33.
19. Сухов, В. Л. (2020). Гнучкі моделі інтеграції AWS з локальними хмарами. *Інформаційні технології*, 15(5), 12-19.
20. Тарасов, В. П. (2021). Автоматизація процесів управління за допомогою AWS та інших хмарних сервісів. *Технологічний прогрес*, 8(2), 50-58.
21. Тимошенко, Л. О. (2020). Аналіз продуктивності інтегрованих хмарних платформ. *Інформаційні системи та технології*, 7(1), 31-39.
22. Ткаченко, І. М. (2020). Моніторинг продуктивності хмарних платформ. *Інновації та хмарні рішення*, 10(3), 45-52.
23. Шевченко, В. І. (2019). Інновації в хмарних платформах: майбутнє ІТ-інфраструктури. *Інноваційний розвиток*, 10(2), 15-22.
24. Голуб, О. Л. (2022). Інноваційні підходи до інтеграції хмарних платформ. *Сучасні технології та обчислення*, 7(5), 40-48.
25. Герасименко, О. В. (2021). Управління даними в мультихмарних середовищах. *Сучасні інформаційні системи*, 9(1), 25-32.

ДОДАТОК А

Програмний код

```
import boto3

from botocore.exceptions import NoCredentialsError, PartialCredentialsError

# AWS Configuration
AWS_ACCESS_KEY = "YOUR_AWS_ACCESS_KEY"
AWS_SECRET_KEY = "YOUR_AWS_SECRET_KEY"
AWS_REGION = "us-west-2"

# Eucalyptus Configuration
EUCALYPTUS_ENDPOINT = "https://your-eucalyptus-endpoint.com"
EUCALYPTUS_ACCESS_KEY = "YOUR_EUCALYPTUS_ACCESS_KEY"
EUCALYPTUS_SECRET_KEY = "YOUR_EUCALYPTUS_SECRET_KEY"

# Initialize AWS Session
def initialize_aws_session():
    try:
        aws_session = boto3.session.Session(
            aws_access_key_id=AWS_ACCESS_KEY,
            aws_secret_access_key=AWS_SECRET_KEY,
            region_name=AWS_REGION
        )
        print("AWS session initialized successfully.")
        return aws_session
    except (NoCredentialsError, PartialCredentialsError) as e:
        print(f"Error initializing AWS session: {e}")
        return None

# Initialize Eucalyptus Session
def initialize_eucalyptus_session():
    try:
        euca_session = boto3.session.Session(
            aws_access_key_id=EUCALYPTUS_ACCESS_KEY,
```

```

    aws_secret_access_key=EUCALYPTUS_SECRET_KEY,
    region_name="eucalyptus",
    endpoint_url=EUCALYPTUS_ENDPOINT
)
print("Eucalyptus session initialized successfully.")
return euca_session
except (NoCredentialsError, PartialCredentialsError) as e:
    print(f"Error initializing Eucalyptus session: {e}")
    return None

```

Launch EC2 Instance on AWS

```

def launch_aws_instance(ec2_client):
    try:
        instance = ec2_client.run_instances(
            ImageId='ami-0abcdef1234567890', # Replace with your AMI ID
            InstanceType='t2.micro',
            MinCount=1,
            MaxCount=1,
            KeyName='your-key-name'
        )
        print(f"Successfully launched AWS instance: {instance['Instances'][0]['InstanceId']}")
        return instance
    except Exception as e:
        print(f"Error launching AWS instance: {e}")
        return None

```

Create S3 Bucket in Eucalyptus

```

def create_eucalyptus_bucket(s3_client, bucket_name):
    try:
        s3_client.create_bucket(Bucket=bucket_name)
        print(f"Successfully created bucket '{bucket_name}' in Eucalyptus.")
    except Exception as e:
        print(f"Error creating bucket in Eucalyptus: {e}")

```

Monitor Resources

```
def monitor_resources(cloudwatch_client):
```

```
    try:
```

```
        metrics = cloudwatch_client.list_metrics()
```

```
        print("Metrics available:")
```

```
        for metric in metrics['Metrics']:
```

```
            print(metric)
```

```
    except Exception as e:
```

```
        print(f"Error retrieving metrics: {e}")
```

```
# Backup Data
```

```
def backup_data(s3_client, bucket_name, file_path, object_name):
```

```
    try:
```

```
        s3_client.upload_file(file_path, bucket_name, object_name)
```

```
        print(f"File '{file_path}' successfully backed up to '{bucket_name}/{object_name}'.")
```

```
    except Exception as e:
```

```
        print(f"Error backing up data: {e}")
```

```
# Main Function
```

```
def main():
```

```
    # Initialize AWS and Eucalyptus sessions
```

```
    aws_session = initialize_aws_session()
```

```
    euca_session = initialize_eucalyptus_session()
```

```
    if not aws_session or not euca_session:
```

```
        print("Failed to initialize sessions. Exiting.")
```

```
        return
```

```
    # Initialize clients
```

```
    aws_ec2 = aws_session.client('ec2')
```

```
    aws_s3 = aws_session.client('s3')
```

```
    aws_cloudwatch = aws_session.client('cloudwatch')
```

```
    euca_s3 = euca_session.client('s3')
```

```
# Launch AWS EC2 Instance
```

```
launch_aws_instance(aws_ec2)
```

```
# Create a bucket in Eucalyptus
```

```
create_eucalyptus_bucket(euca_s3, 'eucalyptus-demo-bucket')
```

```
# Backup file to AWS S3
```

```
backup_data(aws_s3, 'aws-demo-bucket', 'path/to/local/file.txt', 'backup-file.txt')
```

```
# Monitor AWS resources
```

```
monitor_resources(aws_cloudwatch)
```

```
# Run the main function
```

```
if __name__ == "__main__":
```

```
    main()
```

```
import logging
```

```
# Configure logging
```

```
logging.basicConfig(
```

```
    filename="cloud_integration.log",
```

```
    level=logging.INFO,
```

```
    format="%(asctime)s - %(levelname)s - %(message)s"
```

```
)
```

```
# Auto Scaling in AWS
```

```
def configure_auto_scaling(asg_client, launch_configuration_name, auto_scaling_group_name):
```

```
    try:
```

```
        # Create launch configuration
```

```
        asg_client.create_launch_configuration(
```

```
            LaunchConfigurationName=launch_configuration_name,
```

```
            ImageId='ami-0abcdef1234567890', # Replace with your AMI ID
```

```
            InstanceType='t2.micro',
```

```
            KeyName='your-key-name'
```

```
)
```

```
        logging.info("Launch configuration created successfully.")
```

```

# Create auto-scaling group
asg_client.create_auto_scaling_group(
    AutoScalingGroupName=auto_scaling_group_name,
    LaunchConfigurationName=launch_configuration_name,
    MinSize=1,
    MaxSize=5,
    DesiredCapacity=1,
    VPCZoneIdentifier="subnet-0123456789abcdef", # Replace with your subnet
    Tags=[
        {'Key': 'Name', 'Value': 'AutoScalingInstance', 'PropagateAtLaunch': True}
    ]
)
logging.info("Auto-scaling group configured successfully.")
except Exception as e:
    logging.error(f"Error configuring auto-scaling: {e}")

# Generate Usage Report
def generate_usage_report(cloudwatch_client, namespace):
    try:
        metrics = cloudwatch_client.list_metrics(Namespace=namespace)
        report = []
        for metric in metrics['Metrics']:
            dimensions = ", ".join(
                [f"{dim['Name']}={dim['Value']}" for dim in metric.get('Dimensions', [])]
            )
            report.append(f"Metric: {metric['MetricName']}, Dimensions: {dimensions}")

        logging.info("Usage report generated successfully.")
        with open("usage_report.txt", "w") as report_file:
            report_file.write("\n".join(report))
        print("Usage report saved to 'usage_report.txt'.")
    except Exception as e:
        logging.error(f"Error generating usage report: {e}")

# Monitor Logs and Alerts

```

```

def setup_monitoring_and_alerts(cloudwatch_client, alarm_name, sns_topic_arn):
    try:
        # Create CloudWatch Alarm
        cloudwatch_client.put_metric_alarm(
            AlarmName=alarm_name,
            MetricName="CPUUtilization",
            Namespace="AWS/EC2",
            Statistic="Average",
            Period=300,
            EvaluationPeriods=1,
            Threshold=80.0,
            ComparisonOperator="GreaterThanThreshold",
            Dimensions=[
                {"Name": "InstanceId", "Value": "i-0123456789abcdef"} # Replace with your instance ID
            ],
            AlarmActions=[sns_topic_arn]
        )
        logging.info(f"Alarm '{alarm_name}' created successfully.")
    except Exception as e:
        logging.error(f"Error creating monitoring alarm: {e}")

# Extended Main Function
def main():
    # Initialize AWS and Eucalyptus sessions
    aws_session = initialize_aws_session()
    euca_session = initialize_eucalyptus_session()

    if not aws_session or not euca_session:
        logging.error("Failed to initialize sessions. Exiting.")
        return

    # Initialize AWS clients
    aws_ec2 = aws_session.client('ec2')
    aws_s3 = aws_session.client('s3')
    aws_cloudwatch = aws_session.client('cloudwatch')

```

```
aws_asg = aws_session.client('autoscaling')
```

```
euca_s3 = euca_session.client('s3')
```

```
# Launch AWS EC2 Instance
```

```
instance = launch_aws_instance(aws_ec2)
```

```
# Create a bucket in Eucalyptus
```

```
create_eucalyptus_bucket(euca_s3, 'eucalyptus-demo-bucket')
```

```
# Backup file to AWS S3
```

```
backup_data(aws_s3, 'aws-demo-bucket', 'path/to/local/file.txt', 'backup-file.txt')
```

```
# Configure auto-scaling
```

```
configure_auto_scaling(
```

```
    aws_asg,
```

```
    launch_configuration_name="DemoLaunchConfig",
```

```
    auto_scaling_group_name="DemoAutoScalingGroup"
```

```
)
```

```
# Monitor AWS resources and generate usage report
```

```
generate_usage_report(aws_cloudwatch, namespace="AWS/EC2")
```

```
# Set up monitoring and alerts
```

```
setup_monitoring_and_alerts(
```

```
    aws_cloudwatch,
```

```
    alarm_name="HighCPUAlarm",
```

```
    sns_topic_arn="arn:aws:sns:us-west-2:123456789012:MyTopic" # Replace with your SNS topic
```

```
ARN
```

```
)
```

```
# Run the extended main function
```

```
if __name__ == "__main__":
```

```
    main()
```



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

1

**ДИПЛОМНА РОБОТА
на ступінь вищої освіти магістр
із спеціальності 122 Комп'ютерні науки**

**МЕРЕЖЕВА ІНФРАСТРУКТУРА В ХМАРНИХ СЕРЕДОВИЩАХ НА БАЗІ
ІНТЕГРАЦІЇ AWS ТА EUCALYPTUS**

**Виконав: студент 6 курсу, групи КНДМ-63
Сімонов Антон Юрійович
Керівник: завідувач кафедри Комп'ютерних
наук
д.т.н., професор Гніденко М.П.**

Київ - 2024

2

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ДИПЛОМНОЇ РОБОТИ

Тема	Мережева інфраструктура в хмарних середовищах на базі інтеграції Aws та Eucalyptus
Мета дослідження	розробка методичних основ та практичних рекомендацій щодо створення ефективної мережевої інфраструктури в хмарних середовищах на базі інтеграції AWS та <u>Eucalyptus</u>
Наукове завдання	розробка моделі інтегровано мережевої інфраструктури для проведення оцінки за технічними та економічними показниками використовуючи AWS та Eucalyptus
Об'єкт дослідження	хмарні обчислювальні середовища, які функціонують на основі інтеграції публічних і приватних хмарних платформ
Предмет дослідження	є мережева інфраструктура хмарних обчислювальних середовищ із використанням інтеграції AWS та <u>Eucalyptus</u>

СУТНІСТЬ ТА КЛАСИФІКАЦІЯ ХМАРНИХ ОБЧИСЛЕНЬ



Сутність хмарних обчислень

Хмарні обчислення – це модель надання обчислювальних ресурсів (сервери, сховища, програмне забезпечення) через інтернет. Користувачі отримують доступ до ресурсів на вимогу, що забезпечує гнучкість, масштабованість та зменшення витрат на локальну інфраструктуру.

Класифікація хмар

1. **Публічна хмара** – ресурси надаються широкому загалу через інтернет (AWS, Azure).
 2. **Приватна хмара** – ресурси використовуються однією організацією для кращої безпеки та контролю.
 3. **Гібридна хмара** – поєднання публічних і приватних хмар для гнучкого управління навантаженням.
- **Моделі обслуговування**
 - **IaaS** – інфраструктура як послуга (віртуальні сервери, сховища).
 - **PaaS** – платформа як послуга (середовище для розробки додатків).
 - **SaaS** – програмне забезпечення як послуга (готові програми, як-от Gmail).

Хмарні обчислення забезпечують ефективність та доступність сучасних технологій.

ПОРІВНЯННЯ ПЛАТФОРМ AWS ТА EUCALYPTUS

•AWS (Amazon Web Services)

AWS – це глобальна публічна хмарна платформа від Amazon, що надає широкий спектр керованих послуг, зокрема зберігання, обчислення та бази даних. AWS відзначається високою масштабованістю, надійністю та глобальною доступністю завдяки своїй мережі дата-центрів у різних регіонах світу. Основні переваги AWS включають автоматизоване управління ресурсами, велику екосистему сервісів та підтримку для підприємств будь-якого розміру.

•Eucalyptus

Eucalyptus – це програмна платформа для побудови приватних хмар на основі відкритого коду. Вона дозволяє організаціям створювати власну інфраструктуру для обчислень, сумісну з API AWS. На відміну від AWS, Eucalyptus надає повний контроль над хмарою, що дозволяє розгорнути рішення у власних дата-центрах. Це оптимальний вибір для компаній, які потребують підвищеної безпеки та контролю над даними.

•Основні відмінності:

1. **Доступність:** AWS – глобальна публічна хмара, Eucalyptus – приватна хмара.
 2. **Керування:** AWS пропонує керовані сервіси, тоді як Eucalyptus потребує самостійного адміністрування.
 3. **Гнучкість:** AWS забезпечує автоматизоване масштабування, Eucalyptus – повний контроль та адаптивність для специфічних потреб.
- Обидві платформи мають свої переваги та підходять для різних сценаріїв залежно від вимог організації.



ІНСТРУМЕНТИ ТА МЕТОДИ ІНТЕГРАЦІЇ AWS ТА EUCALYPTUS

Інтеграція хмарних платформ AWS та Eucalyptus дозволяє створювати гібридні середовища, поєднуючи глобальну інфраструктуру AWS із можливостями приватної хмари Eucalyptus. Основними інструментами для такої інтеграції є:

•**API (Application Programming Interface)** – забезпечує стандартизовану взаємодію між платформами, автоматизуючи управління ресурсами та передавання даних.

•**Оркестратори** – інструменти, як-от Kubernetes, які керують контейнеризованими додатками, забезпечуючи розгортання та масштабування в різних хмарних середовищах.

•**Гібридні рішення** – AWS Outposts дозволяє інтегрувати ресурси AWS у локальні дата-центри для узгодженої роботи з Eucalyptus.

Також важливими є інструменти передачі даних (Amazon S3 Transfer Acceleration) та моніторингу (AWS CloudWatch), які забезпечують безпечну та ефективну інтеграцію. Використання методів шифрування, автентифікації та управління конфігураціями підвищує безпеку і стабільність інтегрованих систем.



МОДЕЛЬ ІНТЕГРАЦІЇ AWS ТА EUCALYPTUS

Інтеграція AWS та Eucalyptus

•**Сутність інтеграції:** Поєднання публічної хмари AWS та приватної платформи Eucalyptus дозволяє створити масштабовану та ефективну гібридну інфраструктуру.

•**API та сумісність:** Використання AWS API забезпечує безшовну взаємодію, дозволяючи автоматизувати управління ресурсами на обох платформах.

•**Балансування та масштабування:** AWS Elastic Load Balancing (ELB) і Eucalyptus механізми розподілу навантажень забезпечують стабільну роботу системи навіть під час пікових навантажень.

•**Сховище та резервування:** Eucalyptus Walrus Storage синхронізується з Amazon S3 для зберігання даних та резервного копіювання.

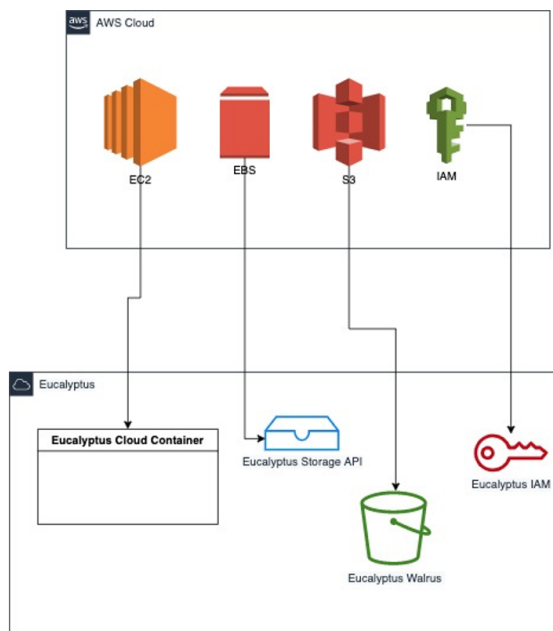
•**Безпека:** Використання AWS IAM та шифрування даних забезпечує захист доступу та конфіденційності інформації.

Переваги інтеграції:

•Контроль над критично важливими даними у приватній хмарі.

•Масштабування ресурсів завдяки AWS.

•Оптимізація продуктивності та витрат.



ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ГІБРИДНИХ ХМАРНИХ СЕРЕДОВИЩ

Гібридні хмарні середовища поєднують гнучкість і контроль приватних хмар із масштабованістю та економічною доцільністю публічних. Такий підхід дозволяє організаціям розміщувати критично важливі дані й сервіси у власних безпечних середовищах, а ресурсоміні та змінні завдання передавати до публічних хмар, забезпечуючи оптимальний баланс між безпекою, дотриманням стандартів та динамічним масштабуванням.

Доступ до передових технологій, що пропонують постачальники публічних хмар, як-от машинне навчання, штучний інтелект чи аналітика великих даних, дозволяє впроваджувати інноваційні рішення без значних капітальних витрат у власну IT-інфраструктуру. Це створює нові можливості для підвищення конкурентоспроможності та ефективності бізнесу.

Таким чином, гібридні хмарні середовища стають фундаментом для адаптивних, гнучких та інноваційних IT-екосистем, які відповідають сучасним вимогам ринку, забезпечуючи безпеку, доступність технологій та безперервність бізнес-процесів.



ВИСНОВКИ

У дипломній роботі досліджено інтеграцію хмарних платформ AWS та Eucalyptus і доведено її вплив на продуктивність, безпеку та економічну ефективність IT-інфраструктури. Завдяки поєднанню масштабованості публічних хмар із контролем приватних середовищ досягається підвищення гнучкості управління ресурсами, оптимізація витрат за моделлю «оплати за використання» та суттєве поліпшення продуктивності мереж. Інтеграція дозволяє знизити затримки та балансувати навантаження, сприяючи кращій обробці великих обсягів даних, а сучасні інструменти для автоматизації мінімізують людський фактор і покращують стабільність. Питання безпеки вирішуються застосуванням сучасних протоколів шифрування та систем управління доступом, а гібридні середовища стають надійним фундаментом для впровадження інноваційних технологій, зокрема штучного інтелекту, IoT та аналітики великих даних. Результати дослідження підтверджують доцільність такої інтеграції для широкого спектра сучасних бізнесів.