Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Факультет комп'ютерних наук
Кафедра теоретичної та прикладної системотехніки

«Затверджую»
Зав. кафедри теоретичної та
прикладної системотехніки
_____ д.т.н., проф. С. І. Шматков
«___» _____ 2024 р

Пояснювальна записка

до кваліфікаційної роботи
бакалавра

на тему: «Мережна інфраструктура гібридної хмарної інформаційної системи»

Захищено на засіданні
Атестаційної комісії № 42
протокол № __ від __.06.2024 р.
Оцінка _____ / _____
Голова Атестаційної комісії
_____ **СКОБ Ю. О.**

Виконала:
студентка 4 курсу, групи КІ–41
Галузь знань: 12 – Інформаційні технології
Спеціальність: 123 – Комп'ютерна інженерія.
КОНЮШЕНКО Поліна Вікторівна

Керівник: професор, д.т.н., професор ЗВО кафедри теоретичної та прикладної системотехніки
АГЄЄВ Дмитро Володимирович

Рецензент: доцент ЗВО кафедри моделювання систем і технологій Факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна
к.ф.-м.н., доц
КАРАСЬ Ірина Вячеславівна _____

Харків – 2024

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи бакалавра складається зі вступу, трьох розділів, висновків, списку використаних джерел і двох додатків. Загальний обсяг роботи складає 68 сторінки, із яких 48 сторінок основної частини з 36 рисунками, 13 найменуваннями списку використаних джерел та двома додатками.

Метою дослідження є розробка та реалізація гібридної хмарної інформаційної системи на основі аналізу існуючих моделей, принципів побудови та технологій розгортання, з метою оцінки її ефективності та визначення практичного та теоретичного значення даної роботи.

Об'єктом дослідження є гібридні хмарні інформаційні системи.

Предметом дослідження є принципи побудови, технології розгортання та архітектура гібридних хмарних інформаційних систем.

Швидкий розвиток інформаційних технологій та збільшення обсягів даних вимагають вдосконалення інфраструктури обчислювальних систем, що робить ***актуальним*** дослідження гібридних хмарних інформаційних систем.

Робота має ***практичне значення,*** оскільки результати дослідження можуть бути використані для розробки та впровадження ефективних гібридних хмарних інформаційних систем у практиці бізнесу та інших сферах діяльності.

Ключові слова: дата центр, хмарні сервіси, гібридна інфраструктура, AWS, технології, модель, сервер.

ABSTARCT

The explanatory note for the bachelor's qualifying work consists of an introduction, three chapters, conclusions, a list of references, and two appendices. The total volume of the work is 68 pages, including 48 pages of the main part with 36 figures, 13 references, and two appendices.

The aim of the research is the development and implementation of a hybrid cloud information system based on the analysis of existing models, construction principles, and deployment technologies, aiming to evaluate its effectiveness and determine the practical and theoretical significance of this work.

The object of the study is hybrid cloud information systems.

The subject of the research is the principles of construction, deployment technologies, and architecture of hybrid cloud information systems.

The rapid development of information technologies and the increase in data volumes require the improvement of the infrastructure of computing systems, making research on hybrid cloud information systems relevant.

The work has practical significance since the research results can be used for the development and implementation of effective hybrid cloud information systems in business practices and other fields of activity.

Keywords: data center, cloud technologies, hybrid infrastructure, AWS, technologies, model.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ..... 5
ВСТУП..... 6
РОЗДІЛ 1. РОЗГЛЯД ПОНЯТТЯ ХМАРНОГО СЕРВІСУ..... 10
1.1 Базові концепції і термінологія..... 10
1.2 Переваги хмари..... 12
1.3 Виклики й ризики..... 14
1.4 Моделі розгортання хмари..... 15
1.4.1 Публічна хмара..... 15
1.4.2 Приватна хмара..... 16
1.4.3 Multicloud..... 17
1.4.4 Hybrid Cloud..... 18
Висновки за розділом 1..... 20
РОЗДІЛ 2. ОГЛЯД ТА ВИБІР ПЛАТФОРМИ ТА ТЕХНОЛОГІЙ..... 21
2.1 Огляд передових хмарних сервісів..... 21
2.1.1 AWS..... 21
2.1.2 VMware..... 21
2.1.3 Microsoft Azure..... 22
2.1.4 Google Cloud..... 22
2.2 Найкращі хмарні надавачі в Україні..... 23
2.3 Огляд технологій та сервісів AWS..... 24
2.3.1 Технології та терміни AWS..... 25
2.3.2 Сервіси AWS..... 26
Висновки за розділом 2..... 28
РОЗДІЛ 3. РОЗГОРТАННЯ ХМАРНОЇ ІНФРАСТРУКТУРИ AWS..... 29
Висновки за розділом 3..... 54
ВИСНОВКИ..... 55
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 56
ДОДАТКИ..... 58
Додаток А..... 58
Додаток Б..... 60
Додаток В..... 65

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

AWS – Веб-сервери Амазон

DNS – Система доменних імен

HTTP – Протокол передачі гіпертексту

HTTPS – Захищений протокол передачі гіпертексту

IAM – Управління ідентифікацією та доступом

NAT – Network Address Translation

RDS – Amazon Relational Database Service

S3 – Simple Storage Service

SSH – Secure Shell

VPC – Virtual Private Cloud

VPN – Virtual Private Network

ВМ – Віртуальна машина

ОС – Операційна система

IP – Internet Protocol

ВСТУП

Центр обробки даних — це потужність обчислень, сховище та програми, необхідні для підтримки корпоративного бізнесу. Інфраструктура центру обробки даних займає центральне місце в архітектурі інформаційних систем, бо через нього проходить вся інформація. Компетентне планування дизайну інфраструктури центру обробки даних з урахуванням потреб продуктивності, відмовостійкості та масштабованості. Крім того, дизайн центру обробки даних має бути гнучким для швидкого розгортання та підтримки нових послуг.

Дата центр - це фізична потуга, яку організації використовують для того, щоб хостити необхідні їм програми та дані. Конструювання дата центрів полягає в тому щоб поєднати обчислювальних ресурсів та ресурсів збереження, які дозволяють давати доступ до потрібних програм і даних. Ключові компоненти конструювання центрів обробки даних можуть бути такими: маршрутизатори, комутатори, шлюзи, брандамауери, системи збереження інформації, сервери та певні системи управління.

Існує багато типів центрів обробки даних та моделей обслуговування. Їх класифікація залежить від того, чи належать вони одній чи декільком організаціям, як вони вписуються (якщо вони вписуються) в топологію інших центрів обробки даних, які технології вони використовують для обчислень та зберігання, а також їхню енергоефективність.

Існує чотири основних типи центрів обробки даних:

1. Центри обробки даних підприємств: Ці центри будуються, належать та експлуатуються компаніями і оптимізовані для їхніх кінцевих користувачів. Зазвичай вони розташовані на корпоративних кампусах.

2. Центри обробки даних з управлінням послуг: Ці центри обробки даних управляються третьою стороною (або провайдером управління послугами) від

імені компанії. Компанія орендує обладнання та інфраструктуру замість їхньої покупки.

3. Центри обробки даних ко-локації: У цих центрах обробки даних компанія орендує простір у центрі обробки даних, який належить іншим і знаходиться поза межами компанії. Центр обробки даних ко-локації господарює інфраструктурою (будівлею, охолодженням, пропускною здатністю, безпекою і т.д.), тоді як компанія надає та керує компонентами, включаючи сервери, сховища та мережеві брандмауери.

4. Центри обробки даних у хмарі: У цій формі центру обробки даних дані та програми розміщуються у постачальниках хмарних послуг, таких як Amazon Web Services (AWS), Microsoft Azure або IBM Cloud, або іншого публічного постачальника хмарних послуг.

Організації можуть вибирати між будівництвом та управлінням власними гібридними центрами обробки даних, орендою простору у центрах обробки даних ко-локації, використанням спільних обчислювальних та сховищевих послуг або використанням послуг, базованих у публічних хмарах. У результаті додатки сьогодні більше не розміщуються лише в одному місці. Вони працюють у кількох публічних та приватних хмарах, управляються пропонованими послугами та традиційними середовищами. У цій епохи мультимодернових центрів обробки даних стали великими та складними, орієнтованими на забезпечення кінцевого користувача найвищою якістю взаємодії.

Мати власний датацентр може мати як переваги, так і недоліки для компанії. Далі розглянемо деякі з переваг.

Контроль над інфраструктурою: Компанія має повний контроль над всіма аспектами датацентру, включаючи обладнання, програмне забезпечення, мережу та безпеку.

Спеціалізована інфраструктура: Власний датацентр дозволяє налаштувати інфраструктуру, щоб вона відповідала унікальним потребам та вимогам компанії.

Безпека даних: Компанія має повний контроль над захистом своїх даних, що може бути особливо важливим для конфіденційної інформації або регульованих даних.

Гнучкість управління ресурсами: Здатність швидко реагувати на зміни в потребах компанії та масштабувати інфраструктуру відповідно до цих потреб.

Далі буде перелічено основні недоліки власних дата центрів.

Високі витрати: Встановлення та утримання власного датацентру може бути дорогим підприємством через витрати на обладнання, енергію, охорону, охолодження та технічну підтримку.

Складнощі у масштабуванні: Розширення власного датацентру може бути складним завданням, особливо якщо потрібно швидко збільшити обсяг обробки даних або об'єм сховища.

Ризик технологічного застаріння: Технології швидко змінюються, і власний датацентр може вимагати постійного оновлення та модернізації, щоб відповідати сучасним стандартам.

Можливі проблеми з безпекою та надійністю: Підтримка високого рівня безпеки та надійності може бути складною задачею, особливо для компаній з обмеженими ресурсами або навичками у цій сфері.

Центр обробки даних - це фізичне приміщення, де організація розгортає IT-інфраструктуру. Він господарює складними засобами зберігання, мережевими та обчислювальними пристроями для безперервної обробки даних. Організації повинні враховувати наступні фактори при проектуванні такого приміщення.

Простір - це площа у квадратних футах або квадратних метрах підлогового простору, який компанія потребує для розміщення своєї IT-інфраструктури. Деякі можуть розділити простір для різних цілей.

Електропостачання включає традиційні, відновлювальні та допоміжні джерела електроенергії, які бізнесу потрібно для безперервної роботи всіх IT-пристроїв без перебоїв..

Обладнання для охолодження, таке як традиційні системи опалення, вентиляції та кондиціонування повітря, блоки управління повітрям в комп'ютерних кімнатах та системи кондиціювання повітря в комп'ютерних кімнатах, запобігають перегріву IT-ресурсів.

Заходи безпеки, такі як електронні замки на дверях, сигналізація, системи відеоспостереження та біометричні сканери, захищають активи від крадіжок та пошкоджень.

Управління будівлею включає електропостачанням, температурою, освітленням, вологістю та реєстрацією безпеки.

Завершуючи обговорення процесів та викликів, пов'язаних з власними датацентрами, необхідно визначити важливість альтернативних підходів у формі хмарних сервісів. Сучасні компанії, стикаючись із зростанням обсягів даних, технологічними змінами та зростаючими вимогами щодо безпеки, знаходять у хмарних сервісах ефективний інструмент для оптимізації своєї інфраструктури та підвищення конкурентоспроможності. Актуальність використання хмарних сервісів у сучасному бізнес-середовищі незаперечна, і дослідження їх потенціалу стає важливим напрямком для подальшого розвитку підприємств у цифрову епоху.

РОЗДІЛ 1
РОЗГЛЯД ПОНЯТТЯ ХМАРНОГО СЕРВІСУ

1.1 Базові концепції і термінологія

Розділ, в якому показується набір базових термінів, які потрібно знати, працюючи з хмарними технологіями.

Хмара означає окреме IT-середовище яке сконструйоване для того, щоб забезпечувати масштабовані і вимірювані IT-ресурси віддалено. Першопочатково цей термін був метафорою до Інтернету, який по суті є мережею з мережами з віддаленим доступом до набору IT-ресурсів. Важливо відділити поняття “хмари” і хмару як символ на позначення Інтернету. Як окреме середовище використовує забезпечення IT-ресурсами віддалено, хмара має чіткі межі. В Інтернеті багато особистих хмар, які доступні через Інтернет. І хоча Інтерет надає відкритий доступ до багатьох IT ресурсів на основі Веб, хмара зазвичай є приватною власністю і пропонує доступ до IT-ресурсів дозовано.

Багато з Інтернету призначене для доступу до заснованих на вмісті IT ресурсів, які опубліковані у Всесвітній Мережі. З іншої сторони, IT ресурси, які забезпечуються хмарою, призначені для забезпечення можливостей обробки бек-енду і доступу користувачів до цих можливостей. Інша ключова відмінність полягає в тому що хмарі не обов’язково бути заснованою на Вебі навіть якщо вони базуються на технологіях та протоколах Інтернет. Протоколи є стандартами та методами, які визначають структуру комунікації між комп’ютерами. Хмара може використовувати будь-які протоколи для забезпечення віддаленого доступу до IT ресурсів.

IT ресурс це фізична чи віртуальний атрибут, який пов’язаний з IT, що може базуватися на програмному забезпеченні, такий як віртуальий сервер чи

кастомна програма чи фізичний або мережевий пристрій, які в свою чергу базуються на апаратному забезпеченні.

On-Premise використовується на позначення IT- ресурсів, які не є хмарними, тобто ті IT ресурси, які розташовуються на підприємстві, в межах організаційної структури традиційним способом, фізично, називаються локальними. Деякі ключові моменти щодо цього поняття: локальні IT ресурси можуть мати доступ до хмарних і взаємодіти з ними, локальний IT ресурс можна перемістити в хмару, тобто зробити з нього хмарний IT ресурс, резервне розгортання IT ресурсів може бути як в локальних так і в хмарних середовищах.

Сторона яка надає хмарні IT ресурси називаються *надавачами хмари*. В сво. чергу сторона, яка використовує ці хмарні IT ресурси являється *споживачем хмари.* Ці терміни описують ролі для організацій, які якимось чином працюють з хмарою.

Масштабування в цій темі означає можливість IT ресурсів справлятися з користувацькими потребами, які збільшуються чи зменшуються. Масштабування може бути вертикальним і горизонтальним.

Горизонтальне масштабування - це коли додаються IT ресурси такого ж типу.

Вертикальне масштабування - це коли IT ресурси заміщаються іншими з потужнішими можливостями. Зазвичай таке масштабування більш дороге, бо потребує спеціалізованих і більш рідкісних серверів, які завжди потребують додаткових налаштувань і обмежені потужностями апаратної частини.

Хмарний сервіс. Не зважаючи на те, що хмара це середовище з віддаленим доступом, не всі розташовані в хмарі IT ресурси можуть бути напряму доступні віддалено. Наприклад, база даних чи фізичний сервер розгорнуті в хмарі, можуть бути доступні лише IT ресурсам, що знаходяться в тій же хмарі. Програма з публічним API може бути розгорнута навмисно для того щоб забезпечити доступ віддаленим клієнтам.

Тобто, хмарний сервіс - це IT ресурс, який може бути доступний лише через хмару.

Еластичністю називають автоматизовану можливість хмари масштабувати IT ресурси, за наперед визначеними умовами від надавача та споживача хмари.

1.2 Переваги хмари

1. Зменшення інвестицій і пропорційність витрат

Надавачі хмари засновують свою бізнес модель на придбанні IT ресурсів у великих обсягах, а потім дають доступ споживачам за більш прийнятною ціною, подібно до продавців, які закуповуються оптом. Це допомагає організаціям мати потужну інфраструктуру без необхідності купувати її самостійно.

Пропорційність витрат полягає в тому, що хмари мають функцію виміру активності споживача і останньому, в свою чергу, треба платити лише за те, що використовується та безпосередньо впливає на ефективність бізнесу. Компаніям не потрібен великий капітал на вкладання в апаратне і програмне забезпечення. Така мінімація початкових фінансових вкладень дозволяє підприємствам починати з малого і за потреби збільшувати кількість IT-ресурсів, що використовуються.

Також надавачі хмари можуть використовувати для розташування своїх потужностей такі місця, де дешевше утримувати нерухомість, необхідних фахівців та пропускну здатність, тож це також призводить до економії витрат.

Загальні переваги споживачів хмари можуть бути наступними:

- короткостроковий доступ до платних обчислювальних ресурсів за потребою та можливість вивільнити їх, коли потреба відпала;

- розуміння того, що можна отримати доступ до необмежених ресурсів в будь-який момент за потреби, дозволяє мінімізувати підготовку до їх використання;

- можливість додавати або прибирати IT ресурси навіть в дрібних деталях (наприклад, прибрати 1 Гб а диску);

- Узагальненість інфраструктури, щоб програми не були прив’язані до пристрою і їх можна легко переміщати;

- також споживачам не потрібно приймати рішення щодо локальних IT ресурсів, бо надавачі хмарних послуг часто надають готові рішення до їх апаратного та програмного забезпечення на різні потреби.

2. Полегшена масштабованість

Хмари можуть швидко та динамічно розподіляти IT ресурси, щоб пристосуватися до хвиль та піків у їх використанні. Тож хмарні IT ресурси звільняються, як тільки вони не потрібні (і за них більше не стягується плата). Це допомагає споживачам (особливо якщо це бізнес) уникнути непередбачуваних втрат в разі сильного навантаження або навпаки, відсутності великої кількості задач.

3. Підвищена доступність та надійність

Ці характеристики дають значну перевагу для бізнесу, оскільки збої в роботі системи, які не обробляються негайно, прямо призводять до втрат клієнтів і прибутку.

Типовою рисою ж хмарних технологій є підвищена доступність IT ресурсів, яка зменшує вплив збою на умови виконання задач. Зокрема, IT ресурси доступні 24/7 та краще обробляють виняткові ситуації, а також швидше відновлюються після відмови.

1.3 Виклики й ризики

Незважаючи на всі вищеописані переваги хмарних технологій, їхні споживачі стикаються з певними викликами при роботі з ними. Проте більшість з них менеджиться, компаніям варто бути чутливими до цих ризиків. Серед них:

- підвищена безпекова вразливість: перемістити дані на хмару означає поділитися ними з надавачем хмари. В такому випадку гадавач має бути готовий чесно говорити про наявні вразливості та/чи проблеми, а споживачеві потрібно попри це довіряти свої дані надавачеві, що може бути складно. Також різні споживачі можуть в різний час користуватися одними й тими ж IT ресурсами, але вимагати від надавача різного ступеню безпеки, що може бути важким для налаштування.

- зменшення урядового контролю над операціями: хмари певною мірою є приватною власністю і стандарти їхньої роботи залежать лише від надавача хмарних послуг. Хоча при заключенні договори надавач дає гарантії споживачеві, останній сам має перевіряти та моніторити чи відповідає фактична якість наданих послуг зазначеним.

- ускладнена портативність: через різні технології у різних надавачів може бути важко перемістити свої дані від одного надавача до другого.

- ускладненя через міжнародний зв’язок: через велику відстань між фізичним розташуванням IT ресурсів і споживачем може бути ненадійний мережевий зв’язок зі стрибками, що призводить до коливання затримки та обмеження пропускної здатності. Споживачі ніколи не знають де саме фізично знаходяться IT ресурси, які вони використовують, тож не можуть прямо контролювати, хто має до них доступ. Також в різних країнах можуть бути різні закони щодо обробки та передачі персональних даних. Але в більшості випадків, якщо з даними щось трапиться відповідальність нестиме сторона компанії споживача.

1.4 Моделі розгортання хмари

Модель розгортання хмари описує такі характеристики як приналежність, доступ та розмір хмарного середовища.

Тож, існує 4 види моделей розгортання: публічна хмара; приватна хмара; мультихмара; гібридна хмара.

1.4.1 Публічна хмара

Public Cloud - вона ж публічна хмара, це таке хмарне середовище, яке належить сторонньому надавачеві хмарних і послуг і є доступним широкому загалу. В публічних хмарах IT ресурси надаються за окрему плату або корціалізуються рекламою чи іншими способами, надаються за допомогою вищеописаних моделей. В публічній хмарі надавач відповідає за створення, безперервну підтримку хмари та IT ресурси які розташовані в ній.

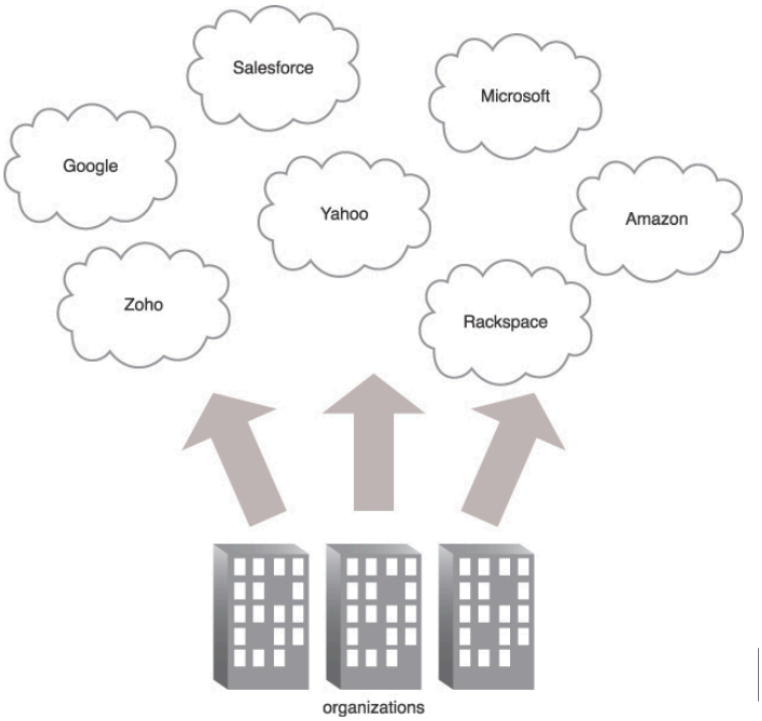


Рис. 1.4 - На малюнку зображені організації-споживачі та деякі головні надавачі публічних хмар, та з’язок між ними.

1.4.2 Приватна хмара

Або ж Private Cloud завжди належить одній організації. Приватнахмара часто створюється як середовище для контролю та певної централізації доступу до IT ресурсів різними департаментами чи іншими частинами однієї організації. Приватна хмара допомагає уникати ризиків та викликів використання хмарних технологій, які були описані раніше, наприклад високий рівень довіри до надавача не так і потрібен, бо в цьому випадку хоч і надвач виступає посередником між IT ресурсами та даними які в них зберігаються, але контроль та управління ними повністю лягає на плечі того, хто створює та налаштовує приватну хмару.

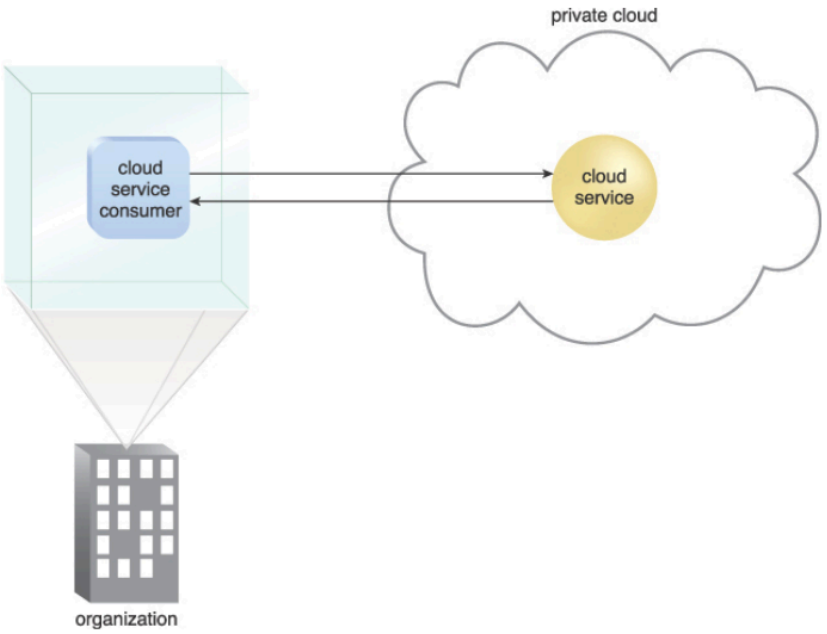


Рис. 1.5. - Приватна хмара

Окремий персонал (який може бути як на аутсорсі, так і всередині компанії у вигляді окремого департаменту тощо), який відповідає за забезпечення хмарою всієї організації бере на себе роль споживача хмарних послуг перед компанією, яка надає інфраструктуру IT ресурсів і роль надавача перед рештою організації.

При роботі з приватною хмарою важливо правильно застосовувати визначення “локальний” і “хмарний”. Не зважаючи на те, що розташування IT ресурсів фізично може бути в приміщенні організації, вони все одно визначатимуться як “хмарні”, бо споживачі з організації будуть мати доступ віддалено

1.4.3 Multicloud

Українською цей термін може бути перекладений як багатохмарність. За допомогою цієї моделі розгортання споживачі хмари можуть користуватися сервісами та IT ресурсами з декількох публічних хмар, як показано на малюнку нижче.

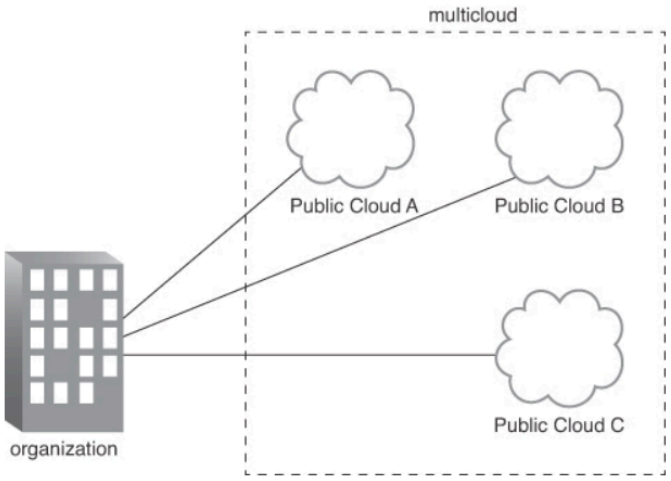


Рис. 1.6 - Мультихмара

Рисунок 1.6 показує як організація користується IT ресурсами від різних надавачів хмари тим самим імплементуючи багатохмарну модель.

Така модель може бути корисною для таких задач як створення резервних копій, покращення переносимості (за рахунок відсутності прив’язаності до одного надавача хмари) або ж специфікація (використання тих публічних хмар, які краще підходять до однієї чи іншої задачі).

1.4.4 Hybrid Cloud

Це таке хмарне середовище, яке поєднує в собі попередньо описані моделі розгортання хмари.

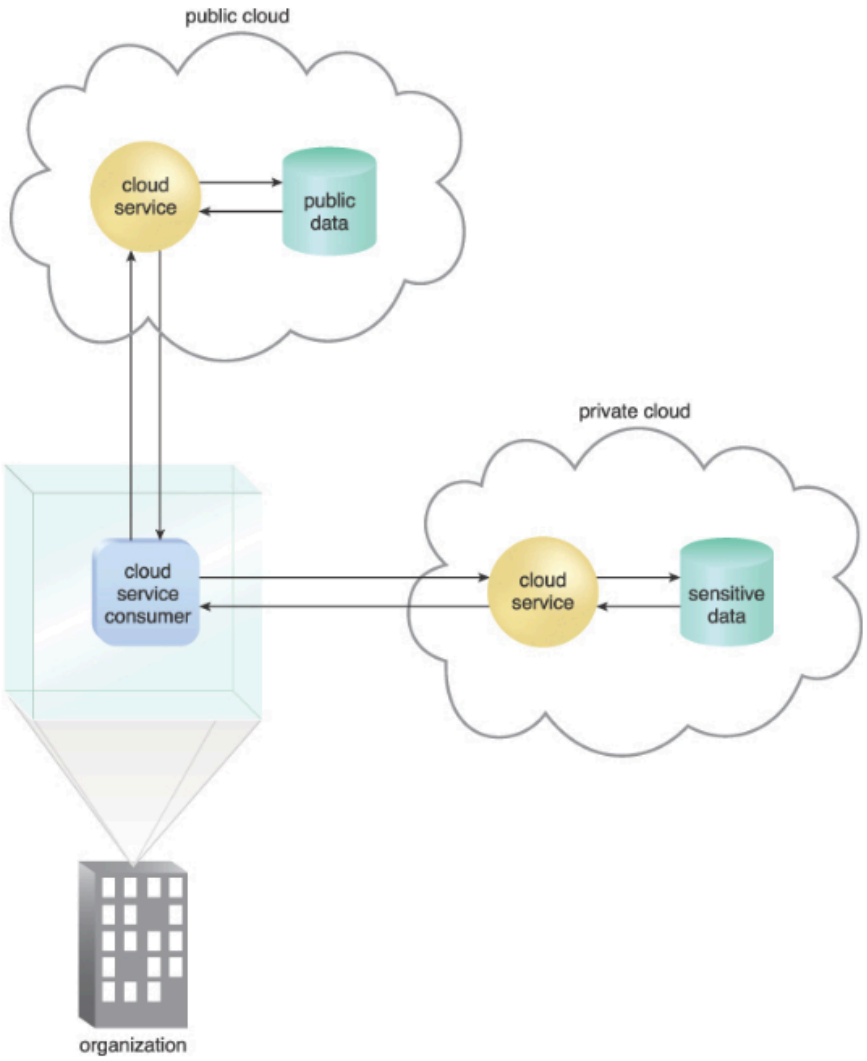


Рис.1.7 - схема мережі, де споживач одночасно використовує публічну (широкодоступну) хмару для загальнодоступної інформації та приватну хмару для чутливої (конфіденційної) інформації.

“Ринок гібридних хмар у 2023 році оцінюється в $129 млрд, а до 2028-го може збільшитися до $348 млрд. Зростаючий попит закономірний, адже хмарні сервіси підвищують ефективність IT-інфраструктури за раціональну

ціну. Розповідаємо, чим саме гібридні хмари корисні для бізнесу та як їх можна використовувати.” [1]

Тож така модель є поєднанням кращих сторін з обох - локальних та хмарних IT ресурсів, яке успішно приміняється для багатьох задач, де покращують перфоманс всі переваги хмарної технології, але іноді потрібна захищеність локального приватного середовища. Наприклад, для збереження чутливих даних, або тестування нових проектів/рис, які не мають заважати основному проекту та експіріенсу клієнтів.

При створенні та використанні гібридної хмарної мережної інфраструктури існують деякі основні ризики й виклики:

Комплексність інтеграції: Інтеграція різних середовищ (локального, хмарного, на краю мережі) може бути складною і вимагати спеціалізованих знань та досвіду для належної настройки та управління.

1. Безпека даних: Передача даних між різними середовищами може створити нові пункти потенційних загроз безпеці. Необхідно впровадити ефективні заходи захисту даних та мереж для запобігання несанкціонованому доступу та втраті інформації.

2. Управління ресурсами та витратами: Ефективне управління ресурсами і витратами у гібридній інфраструктурі може бути складним завданням через розподіленість середовищ та необхідність використання різних інструментів та метрик.

3. Моніторинг і управління продуктивністю: Слід забезпечити ефективний моніторинг та управління продуктивністю усіх компонентів гібридної мережі для забезпечення відповідності вимогам щодо доступності та продуктивності.

4. Відновлення після збоїв: Необхідно мати плани відновлення після збоїв для різних частин гібридної інфраструктури, включаючи локальні, хмарні та розподілені ресурси, щоб мінімізувати вплив можливих виробничих перерв на бізнес-процеси.

Висновки за розділом 1

У розділі детально розглянуті основні терміни, висвітлені переваги використання хмарної інфраструктури, зокрема зменшення інвестицій та підвищення доступності ресурсів. Окрім того, розглянуті переваги короткострокового доступу до обчислювальних ресурсів та можливість їх вивільнення при необхідності.

Проте, разом з перевагами також зазначено й потенційні виклики та ризики. Наприклад, ускладнення портативності даних через міжнародний зв'язок може виникнути при роботі з хмарними сервісами. Також підкреслено підвищену безпекову вразливість, яка може виникнути внаслідок залежності від мережних технологій.

Отже, цей розділ допомагає не лише зрозуміти концепцію хмарних сервісів, але й розглянути їх переваги та можливі ризики, що допоможе прийняти обґрунтоване рішення при впровадженні хмарної інфраструктури.

РОЗДІЛ 2
ОГЛЯД ТА ВИБІР ПЛАТФОРМИ ТА ТЕХНОЛОГІЙ

Розглянемо декілька передових платформ для створення гібридної хмарної інформаційної системи. Насправді це дуже популярна та перспективна галузь на разі, тому навіть при поверхневому дослідженні можна знайти десятки сервісів, які можуть підходити конкретній компанії більше чи менше залежності від її потреб та вимог. На основі цього аналізу оберемо одну, з якою будемо працювати.

2.1 Огляд передових хмарних сервісів

2.1.1 AWS

“Amazon Web Services або AWS (читається як ей дабл ю ес) є дочірньою компанією Amazon.com, що надає платформу хмарних обчислень в оренду приватним особам, компаніям та урядам на основі платної підписки. Існує і безкоштовна підписка, яка доступна протягом перших 12 місяців. Технологія дозволяє абонентам мати у своєму розпорядженні повноцінний віртуальний кластер комп'ютерів, який завжди доступний через Інтернет.”[1]

AWS має величезний список сервісів, деякі з яких я опишу в цій роботі пізніше. Через те що вони сфокусувалися саме на хмарних технологіях і зараз мають глобальну інфраструктуру, з центрами розташованими по всьому світі, що дає доступ широкому колу споживачів легко масштабувати свої додатки/сховища.

2.1.2 VMware

VMware, Inc. (NYSE: VMW) — компанія-розробник програмного забезпечення, найбільш відома продуктами для віртуалізації x86-сумісних комп'ютерів, тобто програмних середовищ, що дозволяють на одному фізичному комп'ютері імітувати роботу кількох віртуальних машин, запускаючи на кожній з них різні операційні системи і застосунки.[2]

VMware, відомий своєю надійністю та широким функціоналом для віртуалізації та управління інфраструктурою, також може використовуватися для створення навчальних мереж у хмарному середовищі. Однак, вартість використання VMware може бути високою через необхідність придбання ліцензій та додаткового обладнання, що робить його менш доступним для малих організацій або проектів з обмеженим бюджетом. Спільний проект VMware Cloud on AWS дозволяє користувачам використовувати засоби VMware в AWS-хмарі, отримуючи доступ до обох екосистем.

2.1.3 Microsoft Azure

“Microsoft Azure («Майкрософт Ежур»), часто згадується просто як Azure — хмарна платформа та інфраструктура корпорації Microsoft, призначена для розробників застосунків хмарних обчислень (англ. cloud computing) і покликана спростити процес створення онлайнових додатків.” [11]

Microsoft Azure, інтегрована з іншими продуктами Microsoft, надає широкий вибір сервісів для розгортання та управління навчальними мережами у хмарному середовищі. Проте, інтерфейс користувача може бути складним для новачків, а вартість використання Azure також може виявитися високою, особливо для великих проектів.

2.1.4 Google Cloud

“Google Cloud Platform — запропонований компанією Google набір хмарних служб, які виконуються на тій же самій інфраструктурі, яку Google використовує для своїх продуктів призначених для кінцевих споживачів, таких як Google Search та YouTube.” [8]

Google Cloud відомий своєю швидкістю та ефективністю, а також інтеграцією з іншими продуктами Google, що робить його привабливим варіантом для створення навчальних мереж у хмарному середовищі. Однак, доступність певних функцій може бути обмеженою порівняно з іншими

хмарними платформами, і підтримка може бути менш доступною для користувачів.

2.2 Найкращі хмарні надавачі в Україні

Загальна ситуація в Україні з такими непереборними чинниками як коронавірусна пандемія та повномасштабна війна тільки прискорили модернізацію компаній та переміщення їхнів ресурсів хмару, адже компаніям треба давати змогу віддаленого доступу до ІТ ресурсів. Особливо компанії зі сходу України, яким важче забезпечувати безпеку фізичних ІТ ресурсів, а також утримувати біля них необхідну кількість персоналу. В 2022 році OSINT агенція Molfar провела дослідження на тему Оцінювались критерії: швидкість підписання угоди, термін надання тестового доступу, ступінь рівня доступу користувача до управління/налаштування наданої інфраструктури, якість роботи техпідтримки тощо.

“GigaCloud (укр. ГігаКлауд) — українська ІТ-компанія, хмарний оператор, що пропонує IaaS (інфраструктура як сервіс) та інші хмарні послуги.”[6]Вони показали найкращі результати з аналізу реакції та умов КП: швидко відповіли на запит, мають гнучку систему знижок/тарифів, відповідає стандарту ISO 27701 з захисту даних (General Data Protection Regulation).

“Лідером за умовами та термінами підписання договору стали Tetcloud з перевагою у швидкості надання договору, а також у додатковому способі оплати “pay as you go” – погодинної оплати за використані ресурси.”[12] На їхньому сайті є калькулятор, який полегшує розрахунок вартості орендованих віртуальних серверів, залежно від їх характеристик.

“З Tucha клієнтам доступні віртуальні сервери гнучких конфігурацій, виділені фізичні сервери в оренду, послуги з хостингу резервних копій, надійне розміщення пошти та сайтів в українських і закордонних дата-центрах, а також хмарне сховище для синхронізації та обміну файлами.”[13] Це лідери в компетентності та зацікавленості фахівців технічної підтримки, а також вони

ведуть канал “Хмарні рішення Tucha”, де на даний момент є вже понад 239 відео з оглядами їхніх сервісів, гайди для споживачів хмарних послуг, відгуки партнерів, інтерв’ю з провідними фахівцями в суміжих галузях, що приємно вразило.

Рис. 2.1 - Порівняльні діаграми лідерів серед хмарних надавачів: загальний рейтинг та за особливими критеріями (з сайту Molfar)

2.3 Огляд технологій та сервісів AWS

Для створення цієї роботи я зупинилась саме на AWS, оскільки вони надають доступ до багатьох сервісів безкоштовно на рік в межах 100$, що дуже зручно для першого знайомства з хмарними технологіями, експериментів та навчальної цілі.

AWS пропонує широкий спектр сервісів для гібридної хмарної інфраструктури, що дозволяє розширювати хмарні ресурси за потребою. Це дозволяє використовувати переваги хмарних сервісів AWS для додатків, які потребують розміщення в певній географічній зоні через обмеження затримки, обсягу даних або вимог до конфіденційності даних. Обравши відповідну архітектуру та сервіси AWS для побудови гібридного хмарного середовища, ми можемо забезпечити бізнесу можливість розгортати ті ж додатки та сервіси незалежно від місця розташування, використовувати однакові інструменти управління та API, а також узгоджувати управління IT операціями, значно покращити продуктивність та ефективність.

2.3.1 Технології та терміни AWS

Аккаунт - обліковий запис, який потрібен для відстеження платежів. Його необхідно мати щоб користуватися сервісами AWS. Різні акаунти можуть бути створені для різних складових бізнесу або різних середовищ.

Регіон - це географічне розташування IT ресурсів, які забезпечує AWS.

Зона доступності - це один або більше центр даних. Регіон створюється з двох або більше зон доступності.Центри обробки даних у зонах доступності підключені один з одним за допомогою високошвидкісного оптоволокна.

AWS сервіси - певні послуги, які може надати AWS.

Публічна підмережа - та, яка підключена до Інтернету відповідним шлюзом.

Приватна підмережа - та, яка не має виходу в Інтернет.

VPN (Virtual Private Network) - технологія від AWS, яка дозволить створити захищене з’єднання між нашою приватною та публічною хмарами. Нижче я наведу деякі інструменти, що використовує ця технологія для найкращого розуміння як ми можемо убезпечити нашу гібридну хмарну інформаційну систему.

Також при створенні акаунту та налаштуванні мережі я використовувала наступні практики щодо безпеки:

Шифрування даних: AWS Key Management Service (KMS) для шифрування даних у стані спокою та під час передачі. AWS KMS дозволяє керувати ключами шифрування, забезпечуючи їх створення, зберігання та керування доступом.

Багатофакторна аутентифікація (MFA): Активація MFA для користувачів IAM для додаткового рівня безпеки.

Групи безпеки (Security Groups) - це станові брандмауери, які контролюють трафік на рівні екземпляра EC2, вони дозволяють або відмовляють у трафіку на основі правил, які визначаються користувачем при створенні, але можуть редагуватися і пізніше.

2.3.2 Сервіси AWS

2.3.2.1 AWS Virtual Private Cloud (VPC) - це сервіс, який надає ізольоване облачне середовище в AWS, де користувачі можуть створювати власні віртуальні мережі з власними IP-адресами, підсітями та таблицями маршрутизації. VPC дозволяє контролювати мережеву конфігурацію, включаючи вибір IP-адресних діапазонів, налаштування доступу до мережі за допомогою списків контролю доступу (ACL) та мережевих маршрутів. Користувачі можуть розгортати віртуальні сервери (EC2), бази даних (RDS), балансувальники навантаження (ELB) та інші ресурси в межах свого VPC. Цей сервіс дозволяє створювати безпечні та ізольовані облачні інфраструктури, що відповідають вимогам безпеки й регуляторних вимог. Він є основою для розгортання різноманітних додатків та служб в AWS, забезпечуючи високий рівень контролю та безпеки над інфраструктурою.

2.3.2.2 AWS EC2 (Elastic Compute Cloud) - це платформа віртуальних обчислювальних ресурсів в рамках Amazon Web Services (AWS), яка забезпечує можливість легко створювати та масштабувати віртуальні сервери, відомі як інстанси, у хмарному середовищі. Користувачі можуть налаштовувати розмір, тип і конфігурацію інстансів залежно від вимог їхніх додатків. EC2 пропонує різноманітні операційні системи, такі як Linux і Windows. Ці інстанси можуть

використовуватися для різних завдань, від простих веб-сайтів до великих обчислювальних кластерів та обробки даних. Завдяки гнучкості масштабування користувачі можуть ефективно використовувати ресурси, змінюючи їх кількість в залежності від потреб. EC2 є ключовим компонентом для швидкого розгортання та масштабування додатків та сервісів у хмарному середовищі.

2.3.2.3 AWS RDS (Relational Database Service) - це керована служба баз даних в хмарному середовищі AWS, що спрощує розгортання, керування та масштабування реляційних баз даних. Вона підтримує популярні системи управління базами даних, такі як MySQL, PostgreSQL, Oracle, SQL Server та інші. Amazon RDS автоматизує багато аспектів, таких як резервне копіювання, патчі, моніторинг, забезпечуючи надійність та високу доступність даних. Користувачам не потрібно проводити складні налаштування, оскільки Amazon RDS надає готове середовище для роботи з даними. Це дозволяє фахівцям зосередитися на розробці додатків, замість витрачання часу на адміністрування баз даних. Завдяки своїй гнучкості та масштабованості, Amazon RDS є привабливим вибором для різних проектів, незалежно від їхнього обсягу та складності.

2.3.2.4 AWS Identity and Access Management (IAM) є сервісом, що забезпечує безпечне та гнучке управління ідентифікацією та доступом до ресурсів AWS. Він дозволяє контролювати, хто має доступ до AWS, які дії можуть вони виконувати та на які ресурси вони можуть отримати доступ. Головні компоненти включають користувачів, групи, ролі, політики та умови, які спільно допомагають налаштувати точні права доступу та забезпечити безпеку даних. Крім того, сервіс надає можливість аудитування дій користувачів для відстеження їхньої активності в системі.

Висновки за розділом 2

У розділі запропоновано широкий огляд передових хмарних сервісів та технологій, що допомагають визначити найбільш підходящі рішення для конкретних потреб. В розділі зазначено основні хмарні платформи, такі як AWS, VMware, Microsoft Azure та Google Cloud, а також проведено аналіз найкращих місцевих надавачів в Україні на основі відповідного дослідження.

Після огляду ринку перехід до детального розгляду технологій та термінів AWS. У розділі надається опис ключових понять, таких як аккаунт, регіон, зона доступності, публічна та приватна підмережа AWS, а також висвітлено практики безпеки, включаючи AWS Key Management Service, багатофакторну автентифікацію та Security Groups.

Крім того, розглядаються основні сервіси AWS, такі як AWS Virtual Private Cloud, AWS EC2 та AWS RDS, а також AWS IAM. Цей розділ допомагає зрозуміти різноманітні можливості та функціонал платформи AWS, що є ключовим етапом при прийнятті рішення про вибір конкретних технологій для реалізації проекту.

РОЗДІЛ 3
РОЗГОРТАННЯ ХМАРНОЇ ІНФРАСТРУКТУРИ AWS

Згідно вимог, нам потрібно створити хмарну інфраструктуру з такими параметрами:

- IP-адреса для Virtual Private Cloud (VPC) - 192.168.0.0/16;
- VPC має містити загальнодоступну і приватну мережі;
- 300 вузлів у загальнодоступній мережі та 100 в приватній;
- необхідно встановити інтернет-шлюз для зв'язку з мережею Інтернет; потрібно розгорнути веб-сервер і створити групи безпеки для мережної безпеки.

Після аналізу висновок: для цих вимог достатньо двох регіонів у хмарній інфраструктурі. Інформаційна інфраструктура включає веб-сервер і базу даних, які мають різні функції та мережні вимоги. Веб-сервер обслуговує доступ і обробку даних, має багато користувачів і IP-адрес. Тому його рекомендується розмістити ближче до користувачів для зменшення навантаження на мережу і поліпшення якості обслуговування. База даних забезпечує зберігання даних, до яких зазвичай звертається веб-сервер, що зменшує кількість IP-адрес для обміну даними і навантаження на мережу.

Зважаючи на попереднє, рекомендується розташувати вебсервер і сервер баз даних у різних зонах доступності (Availability Zone - AZ): вебсервер - у територіально близькій до користувачів AZ, а сервер баз даних - у максимально захищеній. В кожній AZ потрібно створити підмережі та відповідні групи безпеки. Так, для вебсервера потрібно дозволити доступ за протоколами HTTP, HTTPS і SSH лише з окремої IP-адреси для керування віртуальною машиною, на якій встановлено вебсервер. Для сервера баз даних слід обмежити доступ лише від вебсервера. З метою забезпечення зв'язку з зовнішньою мережею Інтернет створюється інтернет-шлюз (Internet Gateway - IGW). Для веб-сервера

створюється екземпляр віртуальної машини (Elastic Compute Cloud - EC2), на якому встановлюється необхідне програмне забезпечення.

Наступним завданням є розрахунок і вибір діапазонів IP-адрес для кожної з підмереж таким чином, щоб виконувалися вимоги щодо їх ємності. Приватна мережа має містити 100 вузлів (IP-адрес). Для цього достатньо використовувати 7 бітів для частини адреси хоста, що забезпечує 128 комбінацій адрес. У Amazon Web Services деякі IP-адреси в кожній підмережі резервуються для службових потреб, тому можна використовувати лише 122 з 128 можливих комбінацій. Зарезервовані комбінації включають адреси мережі та широкомовної розсилки, що призводить до використання менше 100 адрес. Отже, запропоновано використовувати мережу 192.168.0.128/25 та розмістити адреси у діапазоні від 192.168.0.141 до 192.168.0.240.

Згідно вказівок, публічна мережа має вміщати 300 вузлів (з IP-адресами). Це означає, що для частини адреси хоста використовується 9 бітів, надаючи 512 можливих комбінацій адрес. З цих 512 можливих комбінацій 6 зарезервовані, залишаючи 506 доступних (більше 300, як потрібно за завданням). Таким чином, рекомендується використовувати мережу 192.168.2.0/23, де доступні IP-адреси в діапазоні від 192.168.2.3 до 192.168.3.253. Для мережі, що створюється, IP-адреси вузлів можна взяти з діапазону 192.168.2.10 – 192.168.3.53.

Для забезпечення доступу з приватної мережі до Інтернету рекомендується встановити шлюз NAT (NAT Gateway). Використання цього елементу дозволить вузлам з приватної мережі отримати доступ до Інтернету, залишаючи їх недоступними ззовні.

Діаграма хмарної інфраструктури AWS наведена на рис. 3.1.

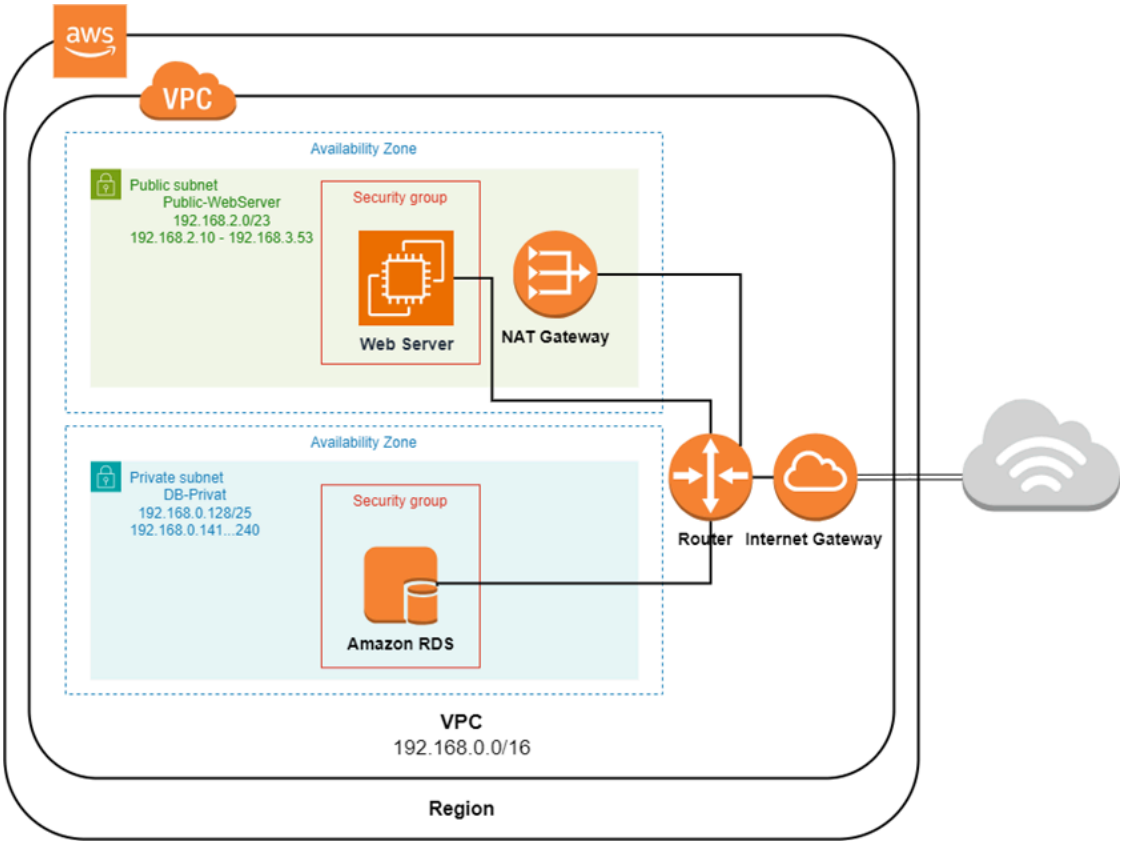


Рисунок 3.1 – Структура хмарної інфраструктури, яка буде розгорнута

Для розгортання описаної інфраструктури необхідно виконати наступні кроки:

– створити віртуальну приватну хмару (VPC);

– створити публічну та приватну підмережу;

– створити інтернет-шлюз та підключити його до віртуальної приватної хмари;

– створити та налаштувати шлюз NAT;

– створити та налаштувати таблиці маршрутизації, підключити їх до підмереж;

– створити та налаштувати групи безпеки;

– створити, налаштувати та запустити віртуальну машину EC2 для вебсерверу у публічній мережі;

– створити, налаштувати та запустити екземпляр сервера баз даних (Amazon RDS).

Для створення віртуальної приватної хмари необхідно відкрити консоль «Amazon VPC», встановити необхідний регіон (US East (N.Virginia)) та натиснути «Create VPC». У панелі, яка з'явиться на екрані (рис. 3.2), необхідно ввести:

– ім'я віртуальної приватної хмари – WebServer-RDS;

– налаштування діапазону IP-адрес.

Інші параметри залишити за замовчанням.

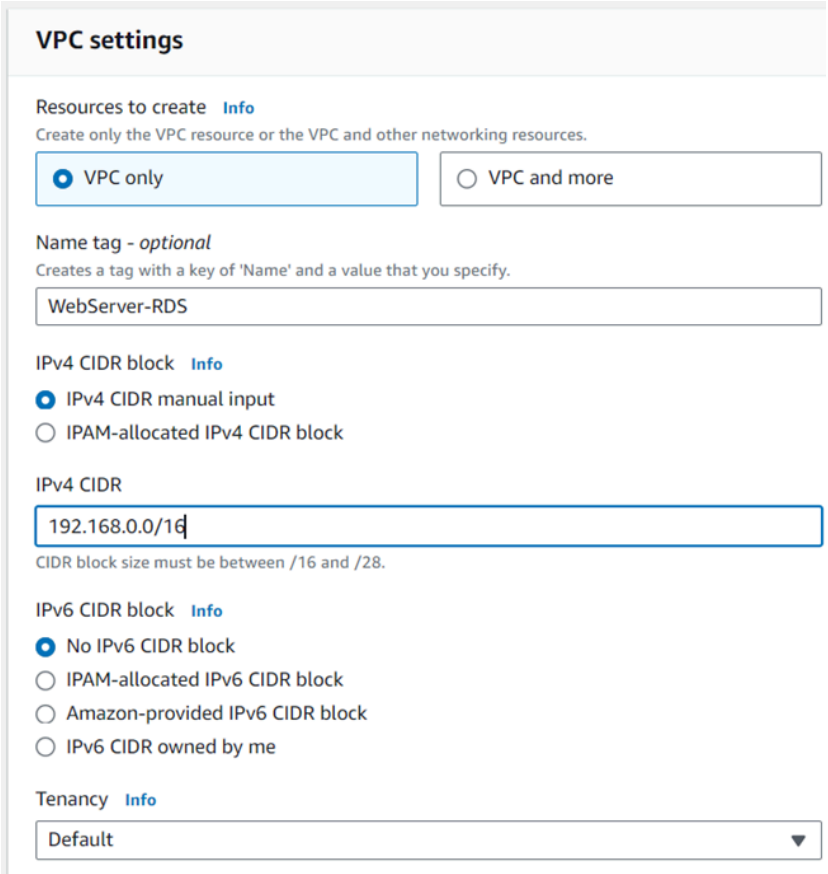


Рисунок 3.2 – Панель створення віртуальної приватної мережі

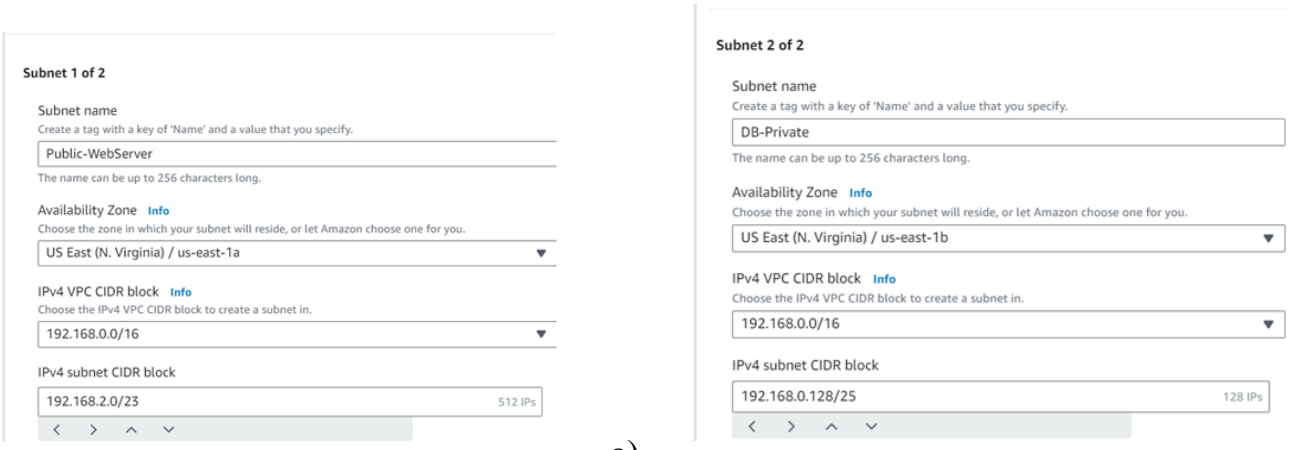
Для створення публічної та приватної підмережі необхідно відкрити консоль «Subnets» та натиснути «Create subnet». У панелі, яка з’явиться на екрані, необхідно зробити наступне:

– у полі «VPC ID» (рис. 3.3) вибрати ім’я віртуальної приватної хмари – WebServer-RDS;

– у панелі налаштування параметрів підмережі (рис. 3.4,а) необхідно вказати ім’я підмережі – «Public-WebServer»; обрати зону доступності – «US East (N.Virginia) / us-east-1a» та налаштування діапазону IP-адрес – 192.168.2.0/23;

– натиснути «Add new subnet» та у панелі, що з’явиться (рис. 3.4,б), вказати аналогічні параметри для приватної мережі: ім’я підмережі – «DB-Private»; зону доступності – «US East (N.Virginia) / us-east-1b» та налаштування діапазону IP-адрес – 192.168.0.128/25.

Рисунок 3.3 – Поле вибору VPC ID



а) підмережа 1 б) підмережа 2

Рис. 3.4 – Панель налаштування підмереж

В результаті у віртуальній приватні хмарі маємо публічну та приватну підмережа у різних зонах доступності (рис. 3.5).

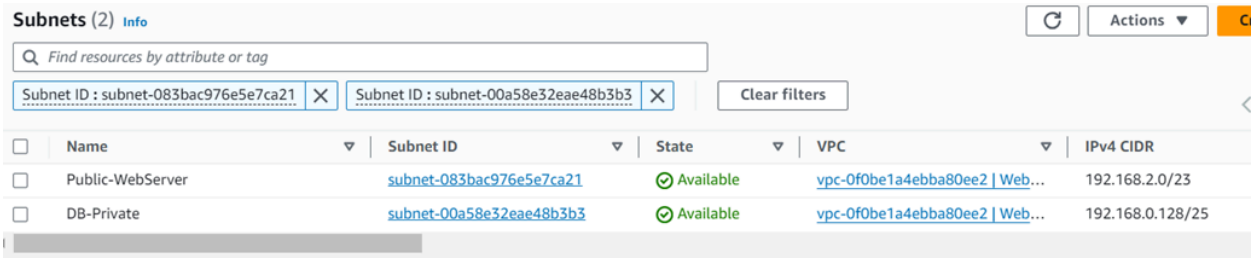
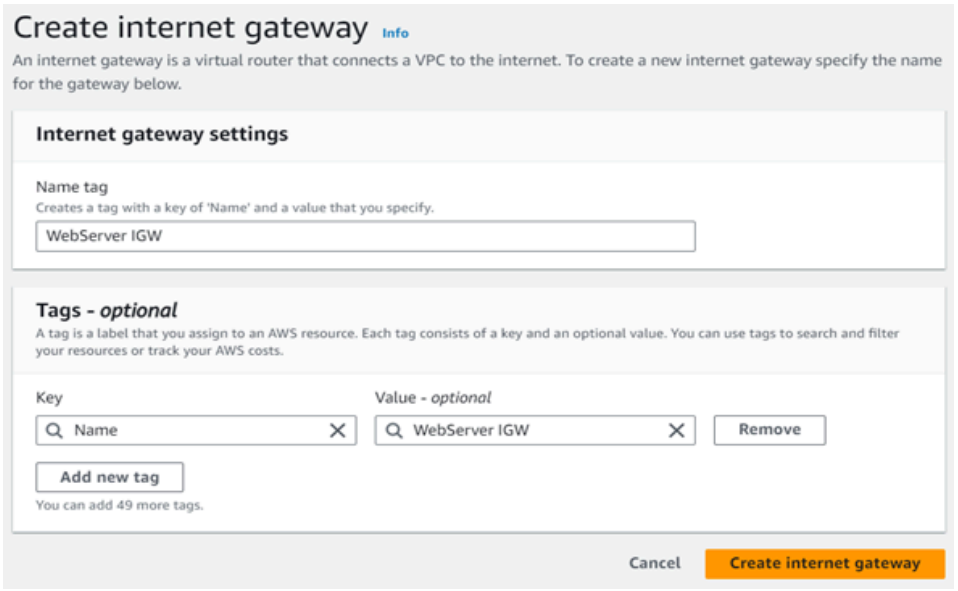


Рис. 3.5 – Створені підмережі

Щоб створити інтернет-шлюз, слід відкрити консоль «Internet gateways» і натиснути «Create internet gateway». У вікні, що з'явиться на екрані (рис. 3.6,а), необхідно ввести назву інтернет-шлюзу – «WebServer IGW» і натиснути «Create internet gateway». Після цього потрібно приєднати інтернет-шлюз до віртуальної приватної хмари. Для цього слід натиснути «Actions» і вибрати пункт «Attach to VPC». У вікні, що з'явиться на екрані (рис. 3.6,б), необхідно для параметра «Available VPC» вибрати назву віртуальної приватної хмари – WebServer-RDS.



а) створення інтернет шлюзу

б) приєднання інтернет шлюзу до VPC

Рис. 3.6 – Створення та налаштування інтернет шлюзу

Для створення шлюзу NAT потрібно відкрити консоль «NAT gateways» і натиснути «Create NAT gateway». У вікні, яке з'явиться на екрані (рис. 3.7), слід:

– ввести назву шлюзу NAT – Public-NAT_GW;

– вибрати підмережу, в якій буде встановлено шлюз – Public-WebServer;

– зазначити тип з'єднання як Public;

– натиснути «Allocate Elastic IP» для створення нового екземпляра для даної публічної IP-адреси;

– натиснути «Create NAT gateway».

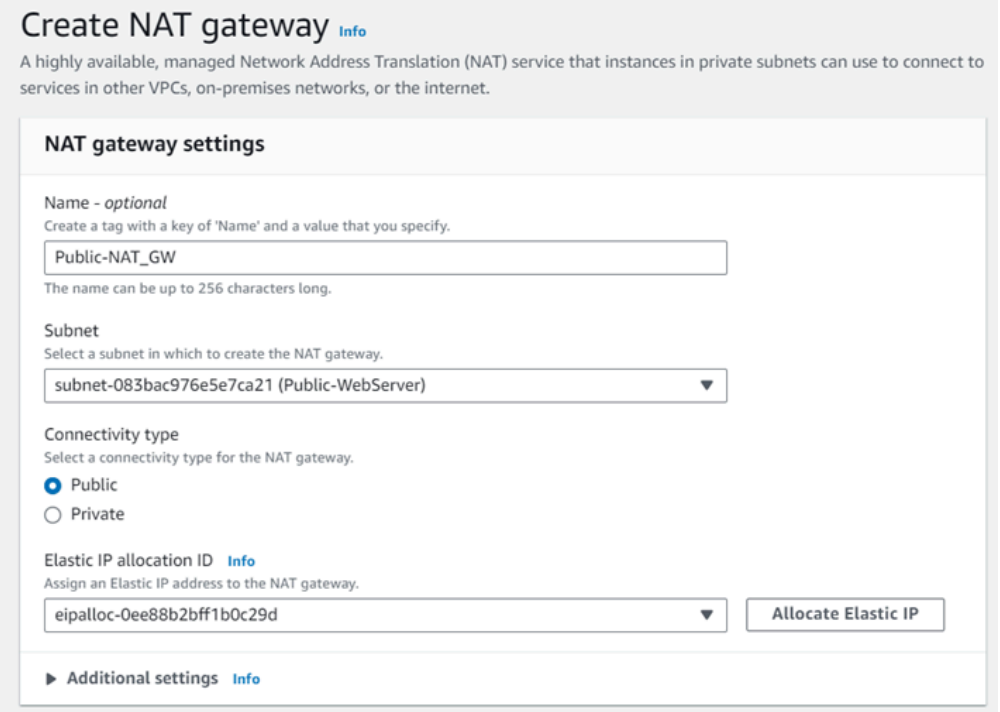
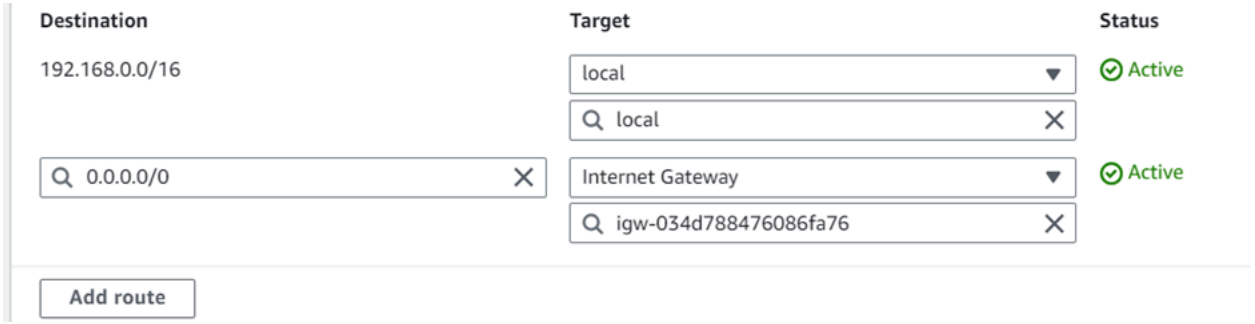


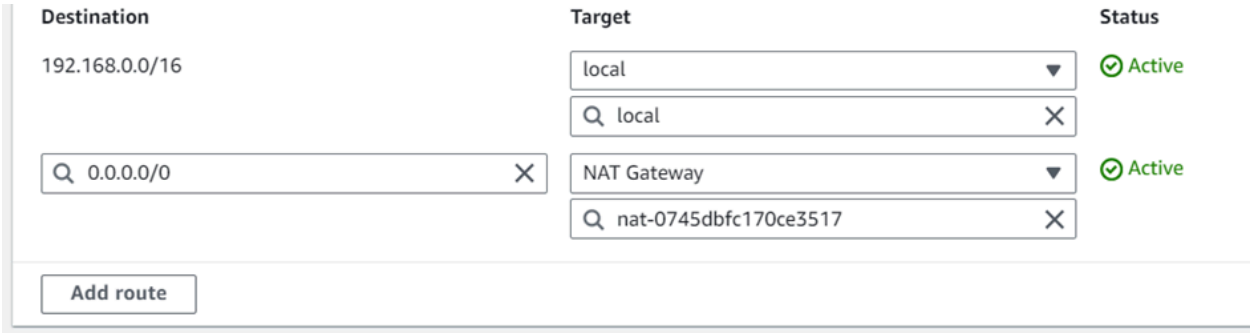
Рис. 3.7 – Інтерфейс для створення та конфігурації шлюзу NAT

Наступним етапом є створення таблиць маршрутизації для публічної та приватної мережі. У розділі «Route tables» потрібно натиснути «Create route table» для створення нових таблиць. Кожну таблицю необхідно назвати відповідно: «Public-Subnet» і «Private-Subnet».

Налаштування маршрутних таблиць ілюструються на рис. 3.8. Слід додати маршрут до інтернет-шлюзу для всіх IP-адрес що не є частиною віртуальної приватної хмари (рис. 3.8,а) щоб реалізувати публічні мережі, а також додати маршрут до шлюзу NAT для приватної мережі (рис. 3.8,б).



а) маршрут до інтернет-шлюзу



б) маршрут до шлюзу NAT

Рис. 3.8 – Конфігураційні панелі таблиць маршрутизації

Наступним кроком буде вхід до консолі «Security groups», щоб створити групи безпеки для веб-сервера та сервера баз даних. У вікні потрібно обрати «Create security group» (рис. 3.9), та ввести подальшу інформацію:

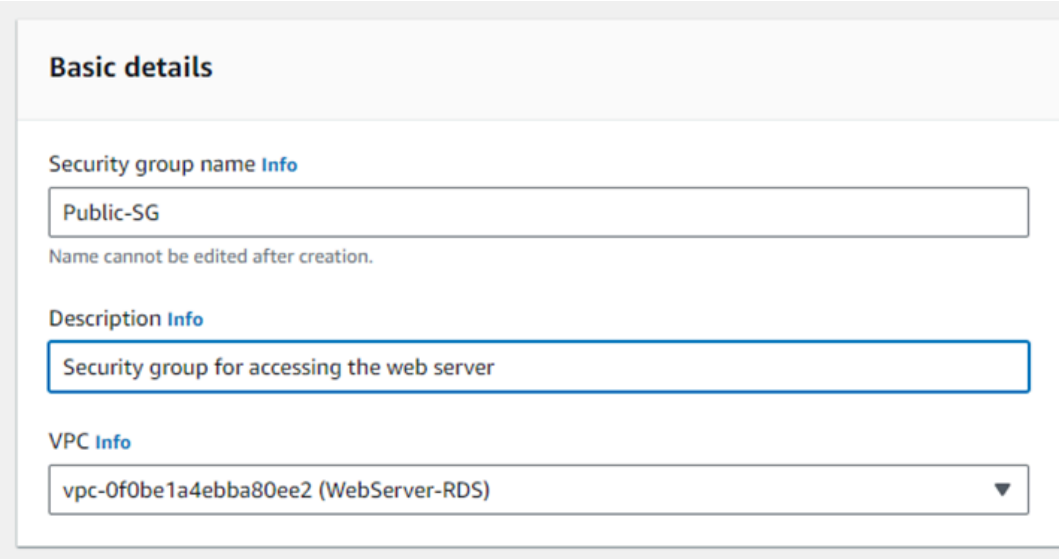
– задати назву групи безпеки – Public-SG;

– ввести опис групи безпеки у розділі «Description»;

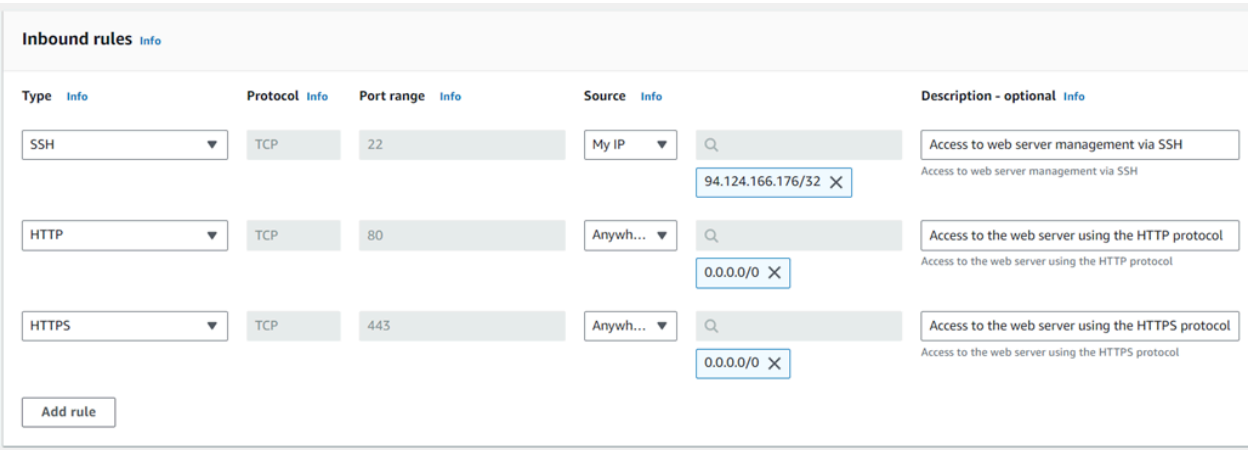
– у розділі «VPC» (рис. 3.9,а) вибрати назву віртуальної приватної хмари – WebServer-RDS.

Користувачам необхідно мати правила доступу через протоколи HTTP та HTTPS. Це можна зробити натиснувши кнопку «Add rule», вказуючи IP-адресу джерела як 0.0.0.0/0, що дозволяє доступ з будь-якої адреси. Також потрібно додати правило, що дозволяє доступ через протокол SSH для керування та налаштування віртуальної машини, на якій розміщено веб-сервер по конкретній

IP-адресі (94.124.166.176/32). Правила для вихідного трафіку не потребують редагування.



а) базова інформація



б) правила безпеки

Рис. 3.9 – Панель налаштування групи безпеки для вебсерверу

Створивши групи безпеки для серверу (рис. 3.10) необхідно:

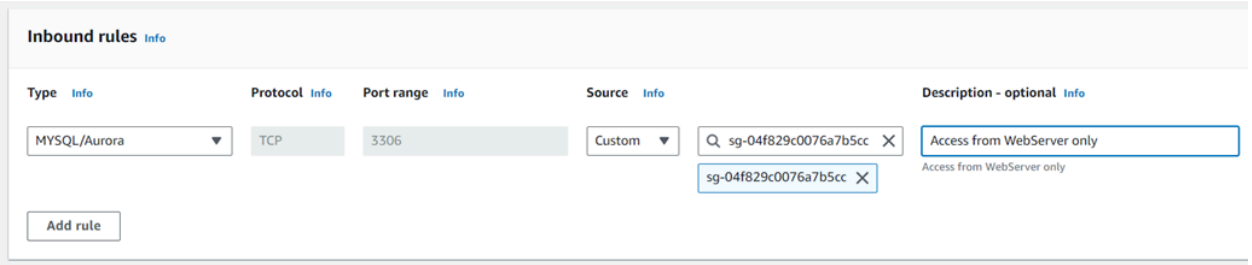
– вписати назву – Private-DB-SG;

– створити опис в полі «Description»;

– Обрати ім’я віртуальної приватної хмари в полі «VPC» – WebServer-RDS. (рис. 3.10,а)

Далі додати правило для вхідного трафіку і обмежити доступ, залишаючи його веб-серверу. Для цього необхідно натиснути кнопку «Add rule» (рис. 3.10,б) і в полі «Type» вибрати протокол – MySQL/Aurora, а в якості джерела вказати групу безпеки – Public-SG (яка відповідає вебсерверу).

а) базова інформація



б) правила безпеки

Рис. 3.10 – Налаштування групи безпеки для сервера баз даних

На останньому етапі в консолі «Amazon EC2» потрібно натиснути «Launch instance». В панелі потрібно вказати ім’я екземпляру – WebServer (рис. 3.11).

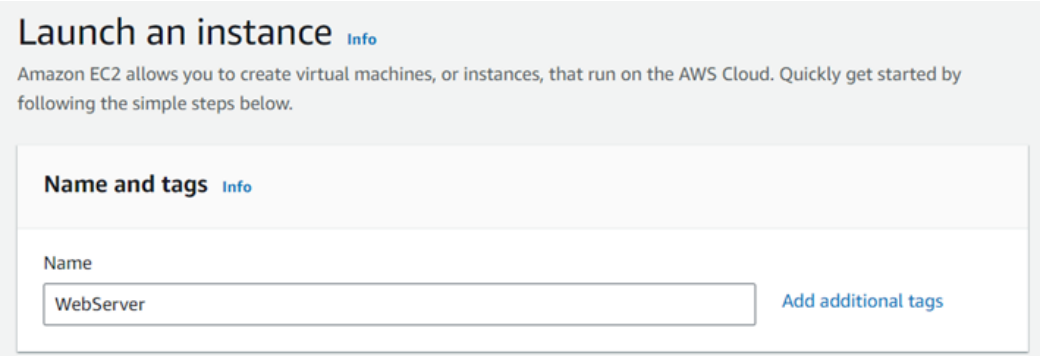


Рис. 3.11 – Встановлення імені екземпляру EC2

Далі потрібно лише вказати Amazon Linux та Amazon Linux 2023 AMI у «Under Application and OS Images (Amazon Machine Image)» (рис. 3.12).

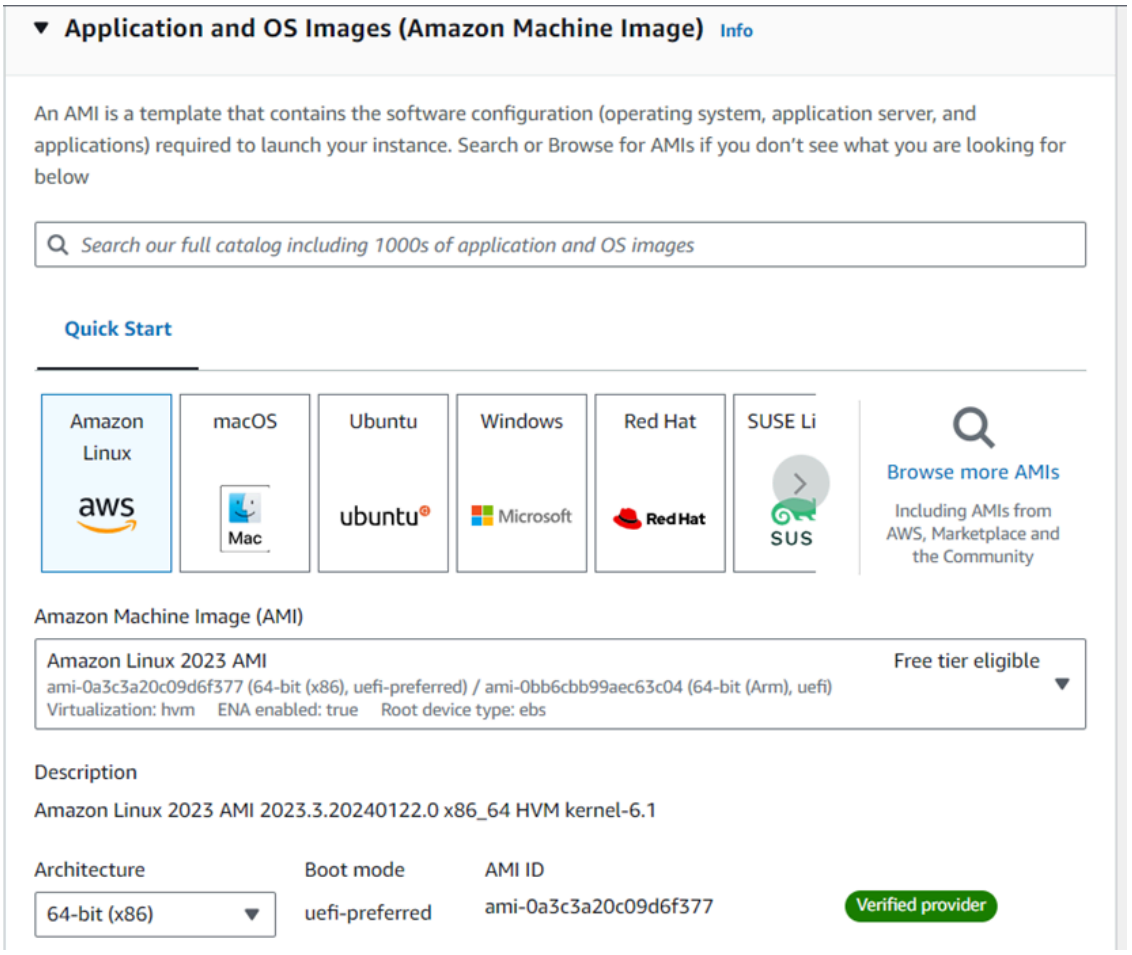


Рис. 3.12 – Вибір операційної системи віртуальної машини

Наступний крок полягає в тому, щоб обрати t3.micro і Diplom-Keys у панелях «Under Instance type» (рис. 3.13) та «Key pair (login)».

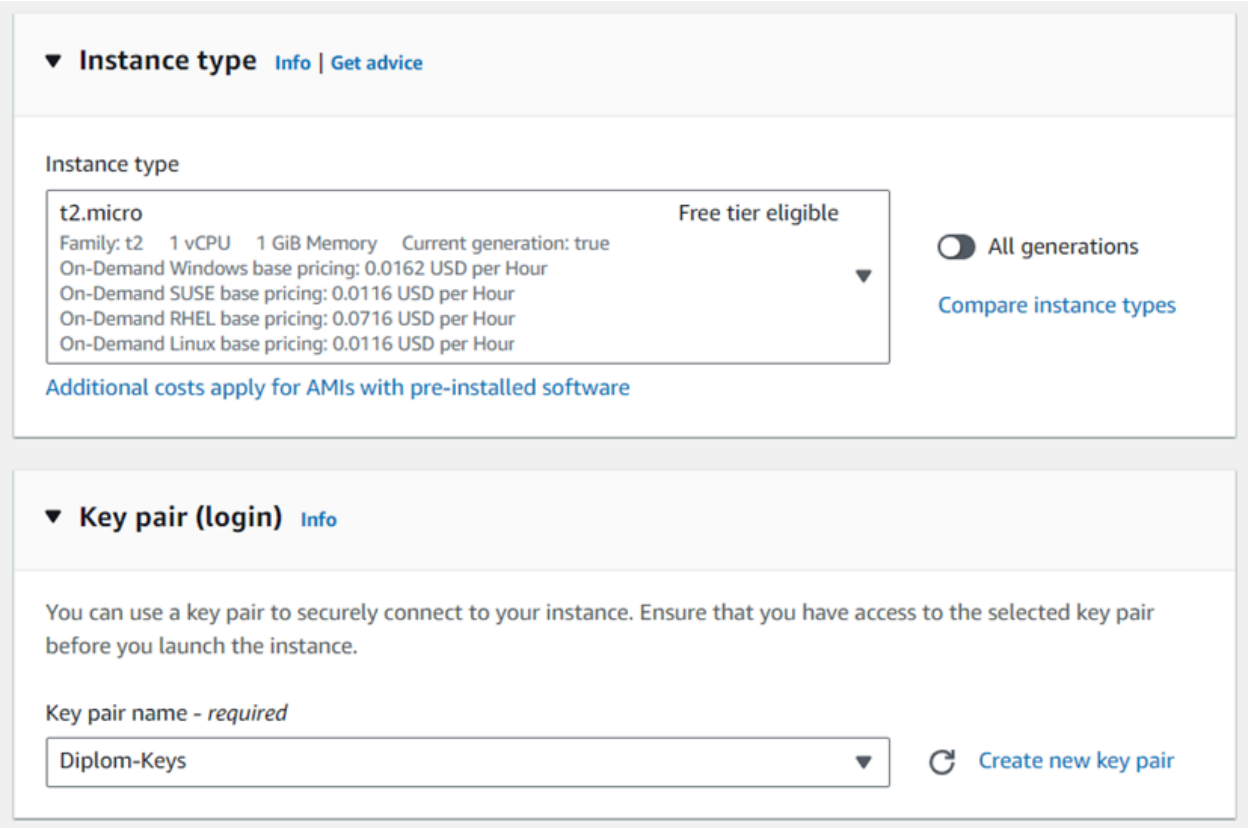


Рис. 3.13 – Налаштування ключа безпеки та екземпляру

Продовжуємо налаштування у панелі «Network settings» (рис. 3.14):

– встановити назву віртуальної приватної хмари в полі «VPC» – WebServer-RDS;

– вказати назву публічної мережі в полі «Subnet» – Public-WebServer;

– обрати «Enable» у полі «Auto-assign public IP», щоб реалізувати авто-призначення публічної адреси;

- вибрати пункт «Select exesting security group», щоб призначити існуючу групу безпеки для вебсерверу – Public-SG.

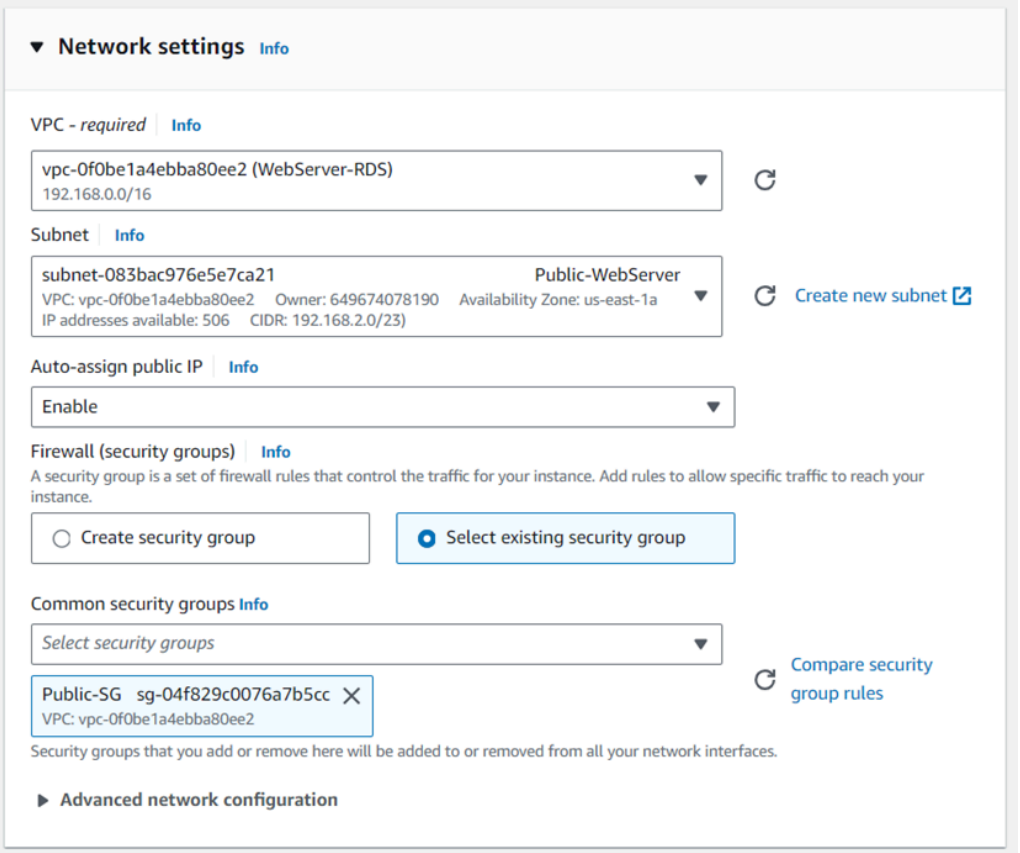


Рис. 3.14 – Налаштування мережі для EC2

Для створення екземпляра серверу баз даних у консолі «Databases» потрібно натиснути «Create database», обрати «Standard create» і тип бази даних MySQL (рис. 3.15).

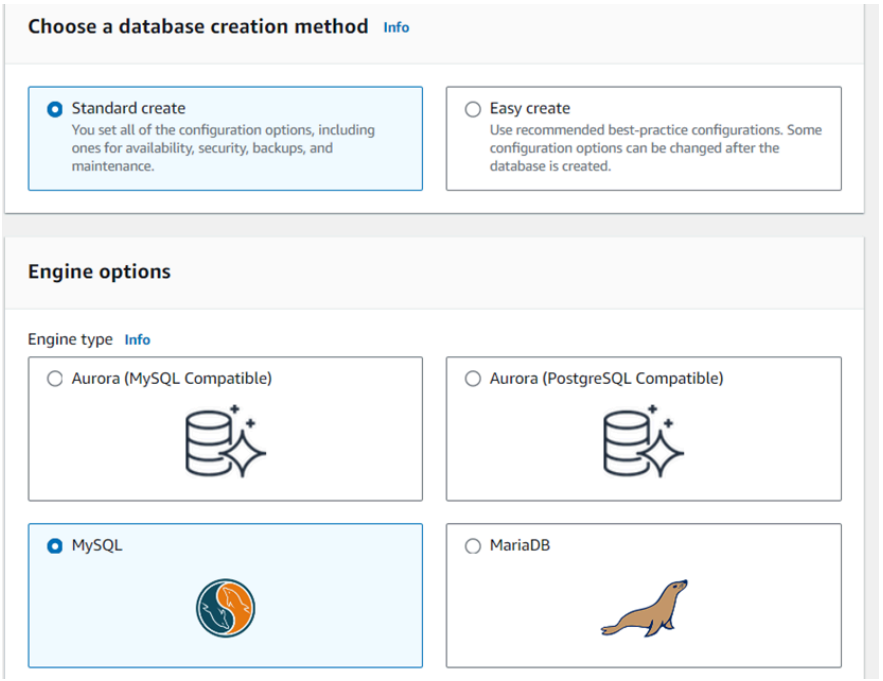


Рис. 3.15 – Стартова панель для створення серверу баз даних

Необхідний шаблон бази даних - «Free tier» (рис. 3.16).

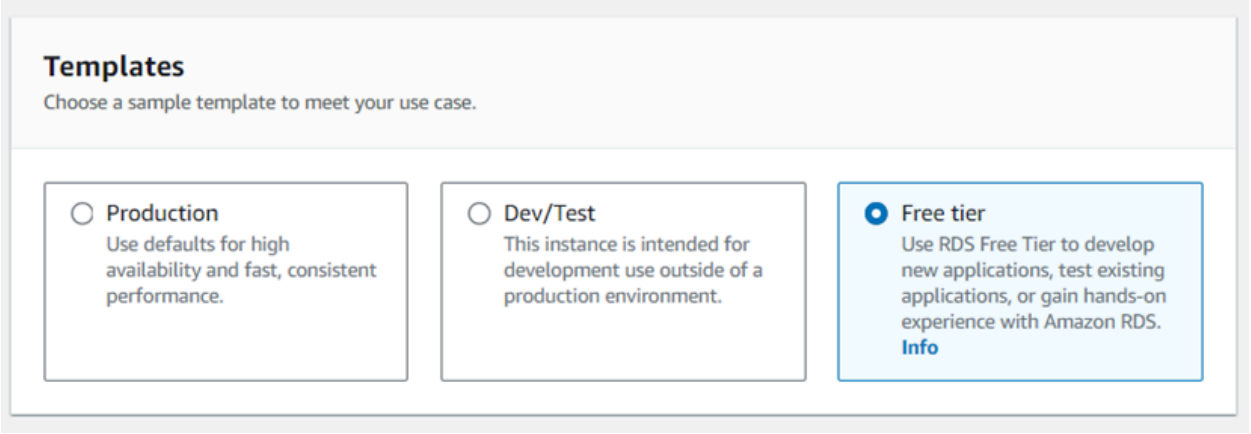


Рис. 3.16 – Панель вибору шаблону бази даних

У секції «Settings» (рис. 3.17) встановіть наступне:

– у полі «DB instance identifier» вкажіть ідентифікатор бази даних – WebServer-DB;

– у полі «Master username» введіть ім'я користувача – admin;

– не відмічайте поле «Auto generate a password»;

– у полях «Master password» та «Confirm password» введіть і підтвердьте пароль.

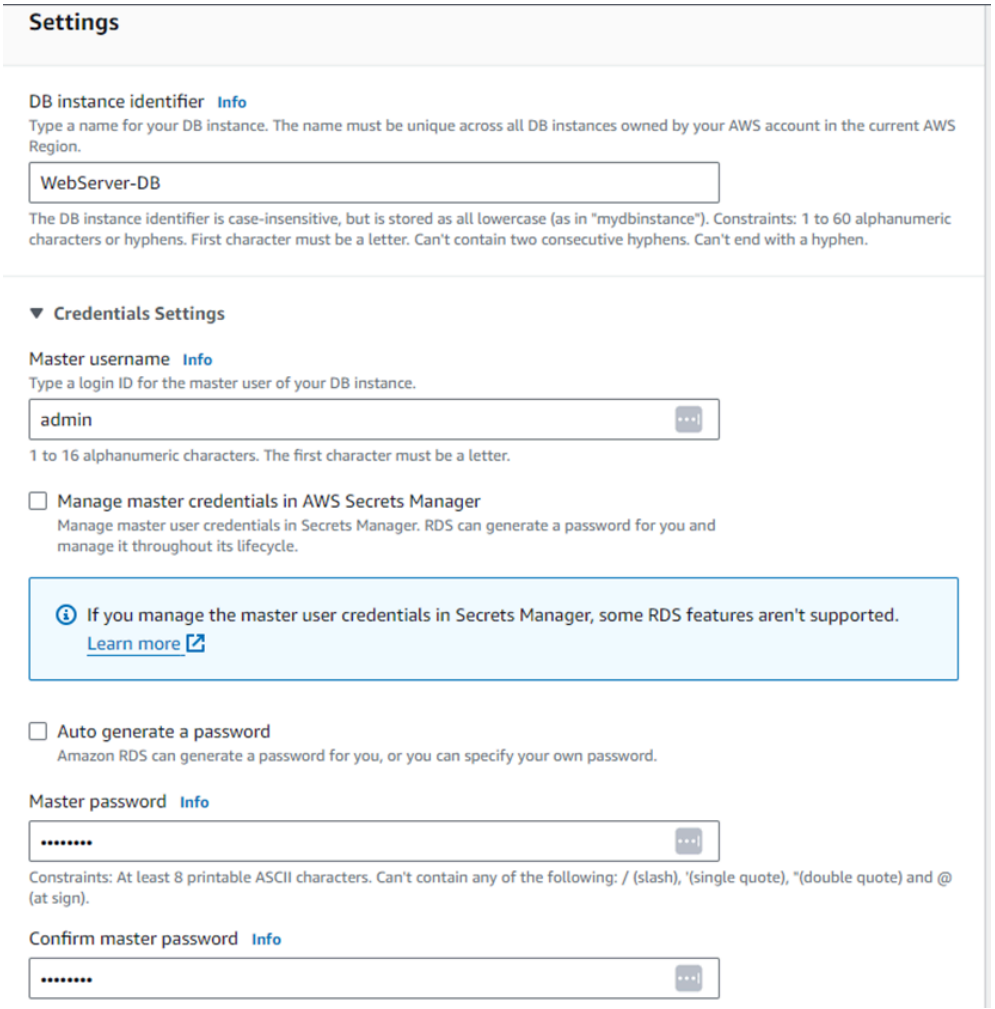


Рис. 3.17 – Налаштування серверу баз даних

У конфігурації екземпляру бази даних (рис. 3.18) встановіть «Burstable classes (includes t classes)» на db.t3.micro для оптимальної продуктивності.

У секції «Connectivity» (рис. 3.19) виберіть «Don’t connect to an EC2 compute resource» для ручного налаштування і зробіть наступне:

– у полі «Virtual private cloud (VPC)» вкажіть WebServer-RDS для правильної мережевої інтеграції;

– у полі «DB Subnet Group» оберіть «Create new DB Subnet Group» для автоматичного створення;

– у полі «Public access» виберіть No, щоб заборонити публічний доступ.

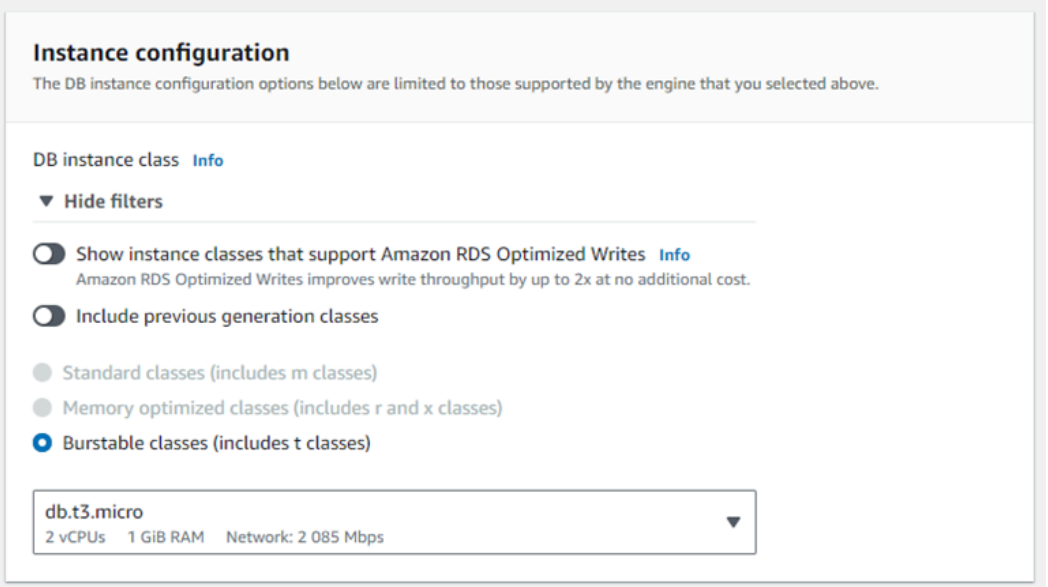


Рис. 3.18 – Конфігурація екземпляру бази даних

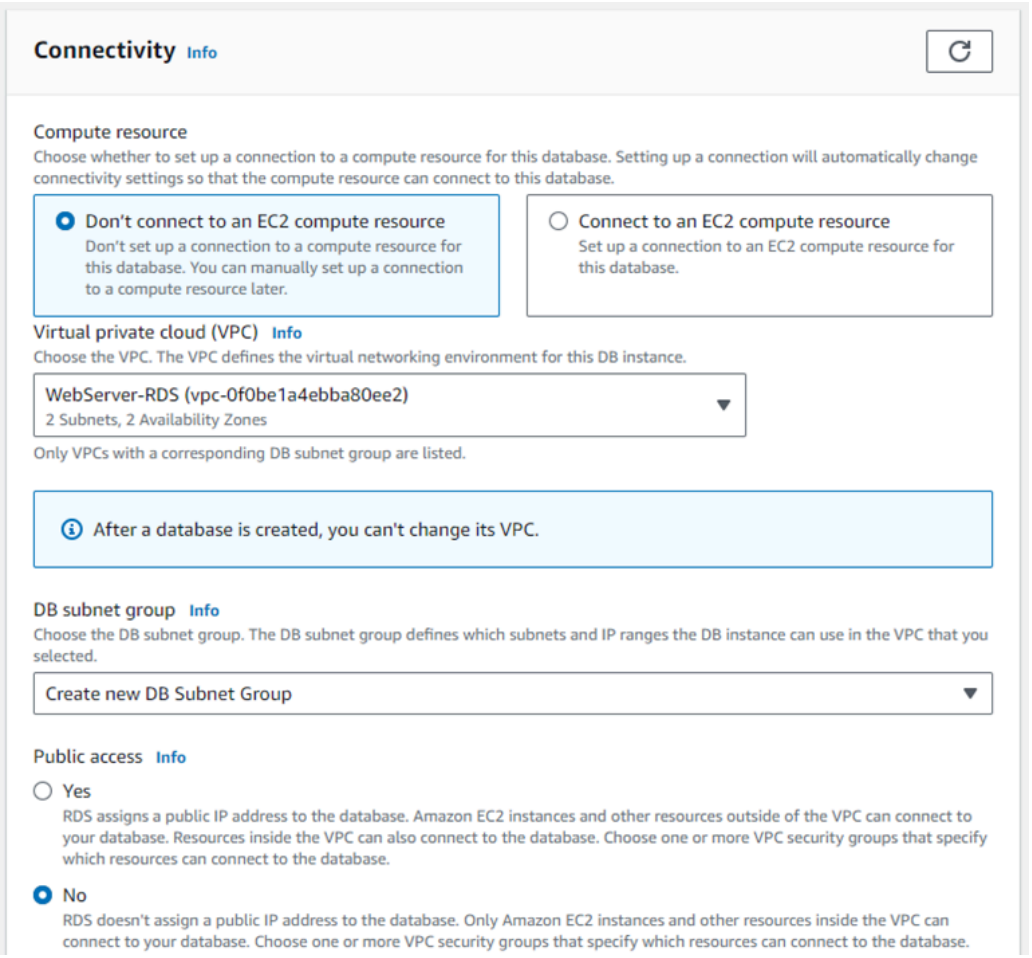


Рис. 3.19 – Конфігурування зв’язку

Додайте до екземпляру бази даних групу безпеки Private-DB-SG та виберіть зону доступності – us-east-1b (рис. 3.20) для оптимального розташування. Інші параметри залиште без змін.

У секції «Database authentication» виберіть опцію Password authentication (рис. 3.21) для забезпечення безпеки.

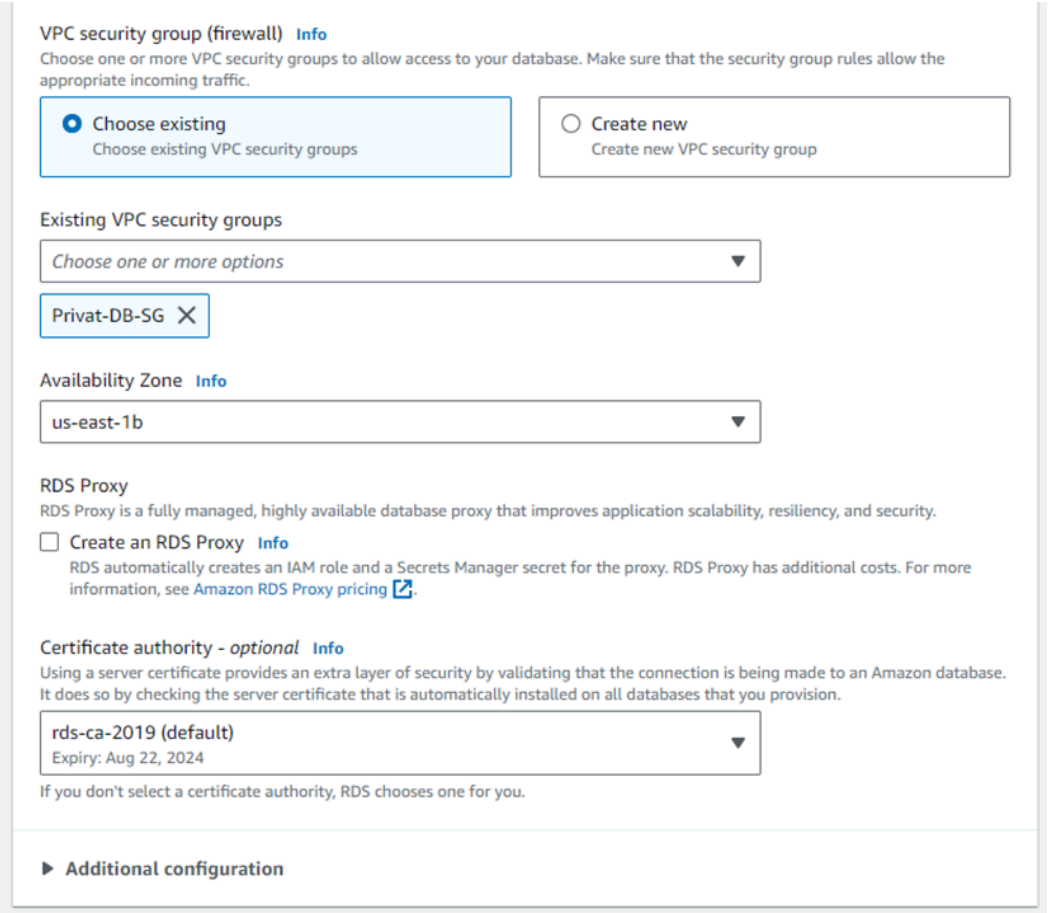


Рис. 3.20 – Налаштування безпеки при з’єднанні

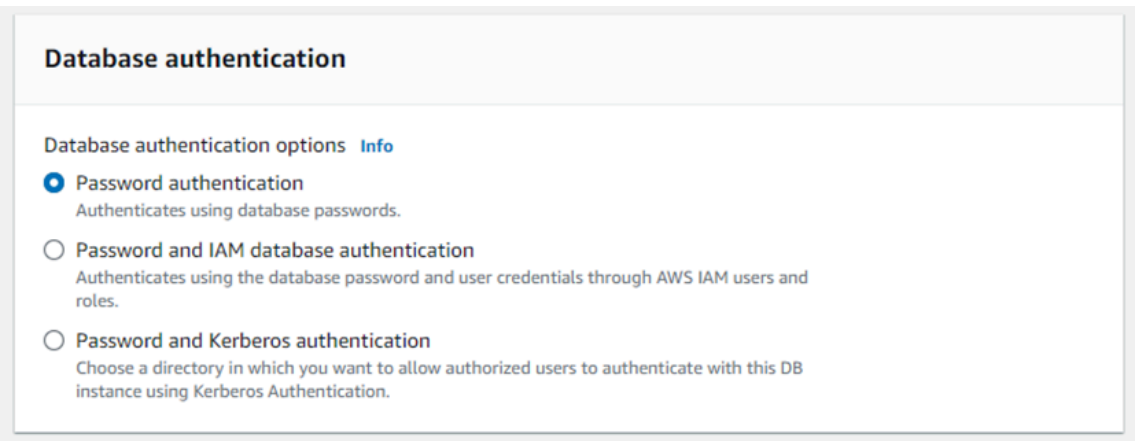


Рис. 3.21 – Секція налаштувань аутентифікації бази даних

У розділі додаткових налаштувань (рис. 3.22) вкажіть назву бази даних як WebServer і натисніть кнопку «Create database», щоб створити та запустити екземпляр.

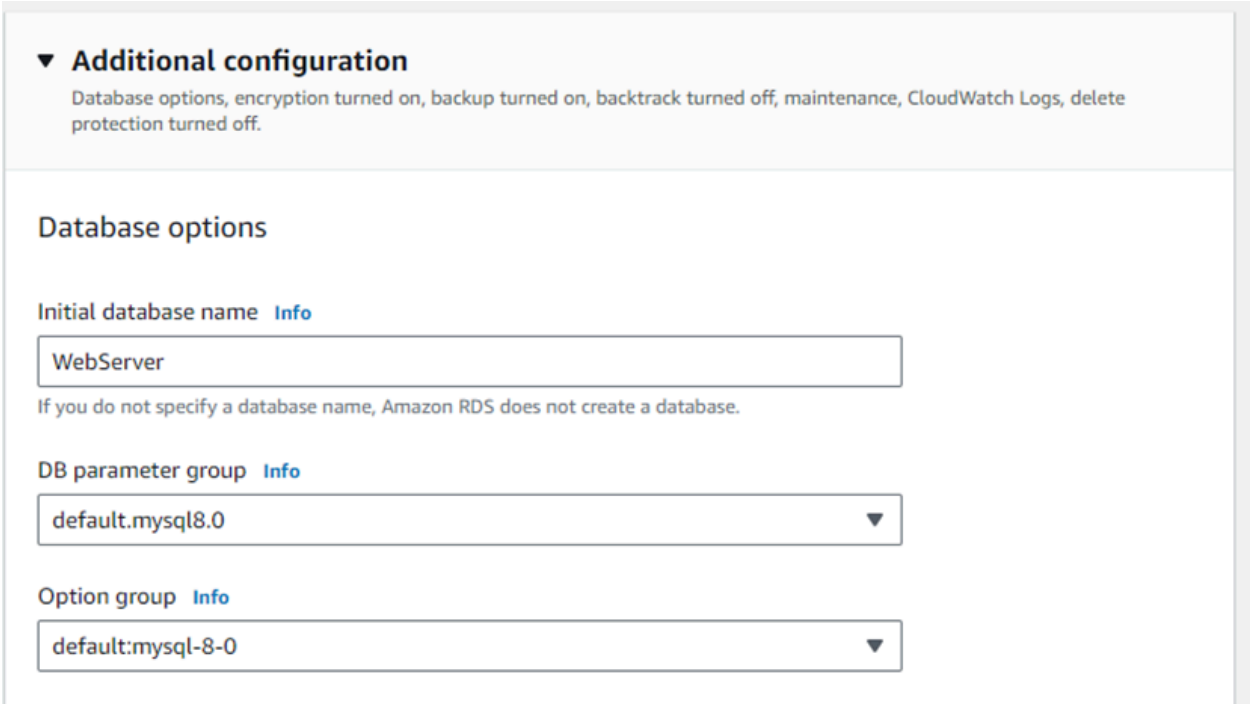


Рис. 3.22 – Секція додаткових конфігурацій

Таким чином маємо інфраструктуру у хмарі AWS, що відповідає вимогам завдання.

Після створення необхідно визначити публічну IP-адресу вебсервера, яку можна знайти в консолі «Amazon EC2» (рис. 3.23) у полі «Public IPv4 address» – це 23.20.9.134.

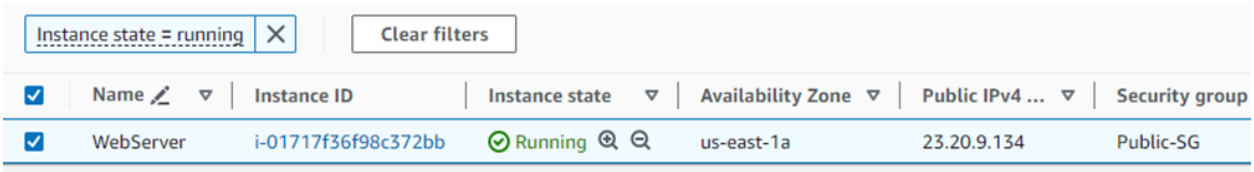


Рис. 3.23 – Інформація про параметри екземпляру вебсерверу

Далі використайте ресурс https://myip.ms/ (рис. 3.24), щоб перевірити IP-адресу. Порівняйте її з IP-адресою, вказаною у налаштуваннях групи безпеки вебсервера.

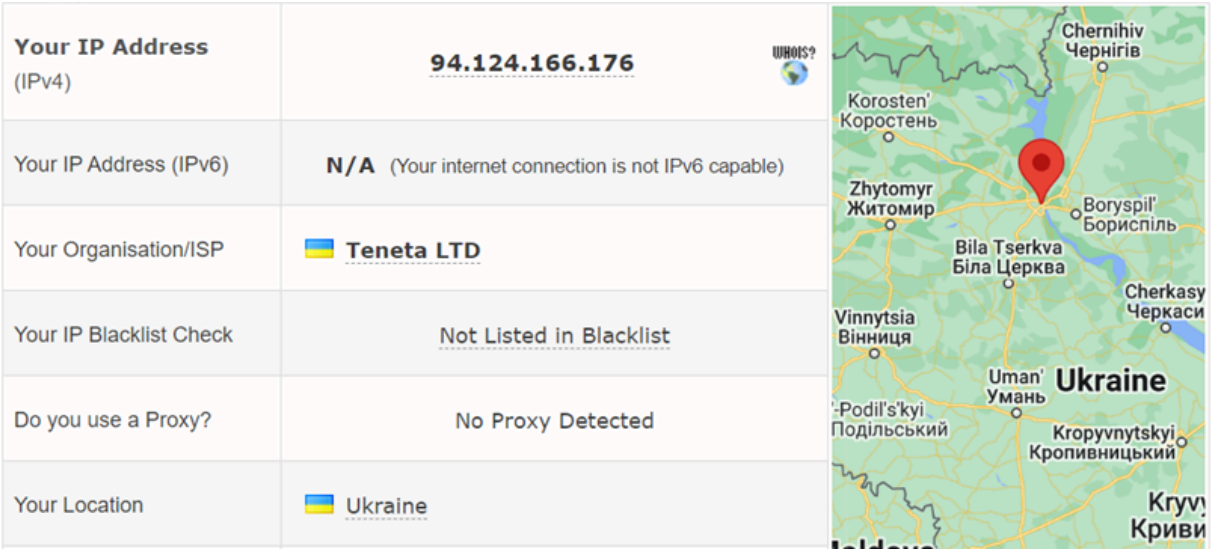
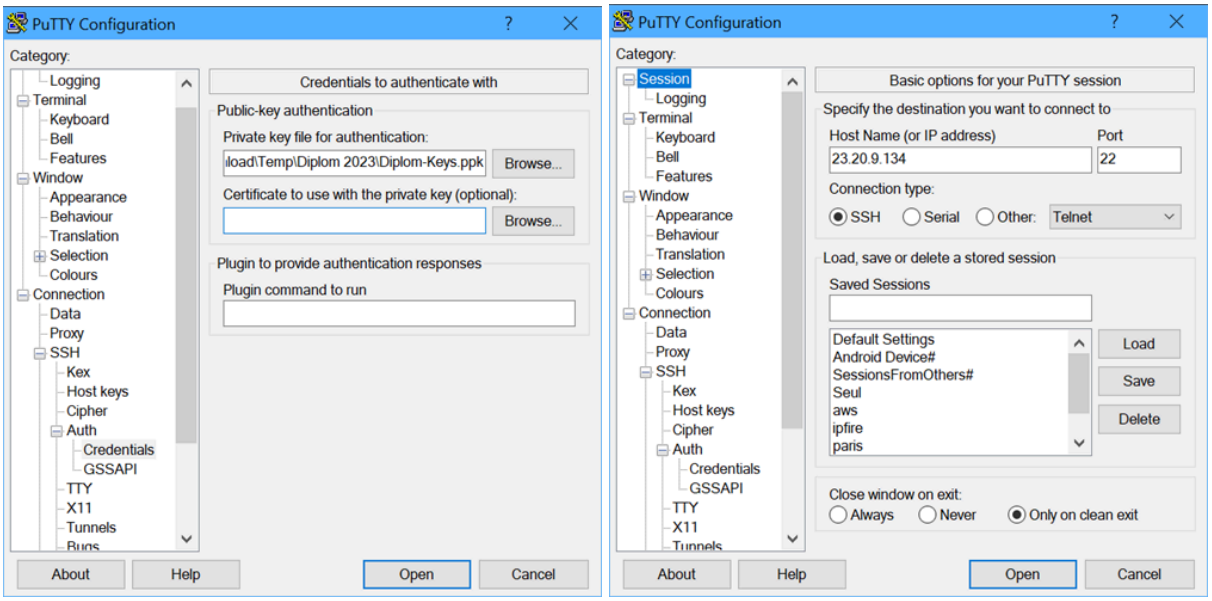


Рис. 3.24 – Визначення власної IP-адреси

Для з'єднання з вебсервером через SSH відкрийте термінал PuTTY (або інший SSH-клієнт), виберіть файл з ключем Diplom-Keys.ppk у панелі автентифікації (рис. 3.25,а). У параметрах з'єднання (рис. 3.25,б) вкажіть публічну адресу вебсервера – 23.20.9.134 і натисніть «Open».

Після успішного з'єднання (рис. 3.26) за протоколом SSH введіть логін – ec2-user. Завершіть з'єднання командою exit в терміналі. Успішне виконання цих дій свідчить про доступність вебсервера для управління через SSH.



а) панель автентифікації б) параметри з'єднання

Рис. 3.25 – Налаштування терміналу PuTTY

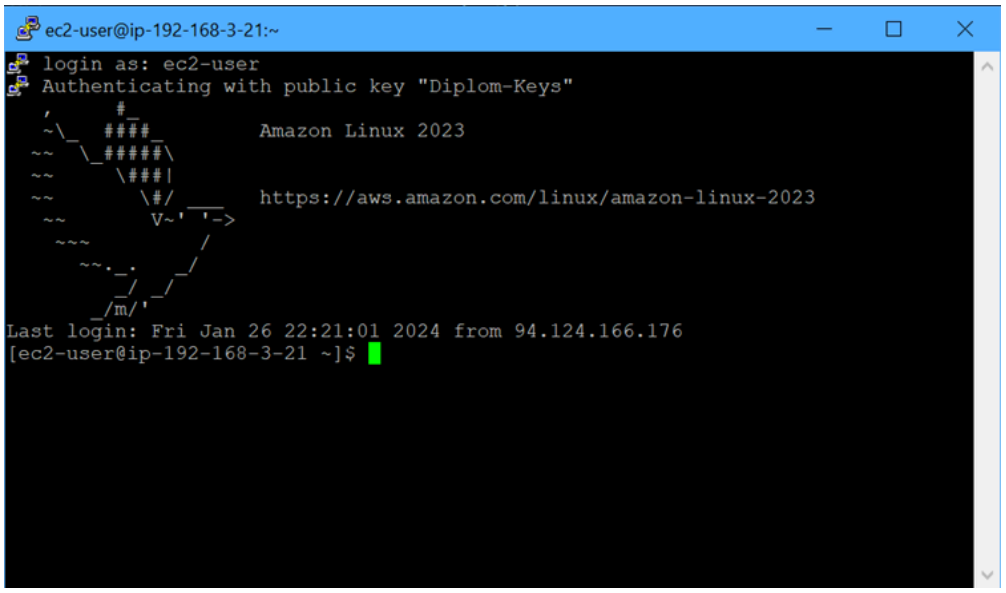


Рис. 3.26 – Вікно терміналу PuTTY після вдалого з’єднання

Для перевірки доступності вебсерверу з іншої IP-адреси, потрібно змінити власну IP-адресу, скориставшись VPN-сервісом. Встановіть VPN-з'єднання і знову перевірте власну IP-адресу за допомогою ресурсу https://myip.ms/ (рис. 3.27).

З рисунку 3.27 можна визначити, що після встановлення VPN-з'єднання ваша IP-адреса змінилася і не співпадає з IP-адресою, вказаною в налаштуваннях групи безпеки вебсерверу.

Your IP Address (IPv4)	**N/A** (Your internet connection is not IPv4 capable)
Your IP Address (IPv6)	**2a01:4f8:13b:4a5:662::1**
Your Organisation/ISP	**Hetzner Online GmbH**
Your IP Blacklist Check	Not Listed in Blacklist
Do you use a Proxy?	No Proxy Detected
Your Location	Germany, Baden-Württemberg, Heidelberg

Рис. 3.27 – Визначення IP-адреси після підключення VPN

Спробуйте встановити з'єднання з вебсервером через SSH знову, використовуючи термінал PuTTY (або аналог). Після зміни IP-адреси (встановлення VPN) з'єднання має бути невдалим (рис. 3.28). Вимкніть VPN.

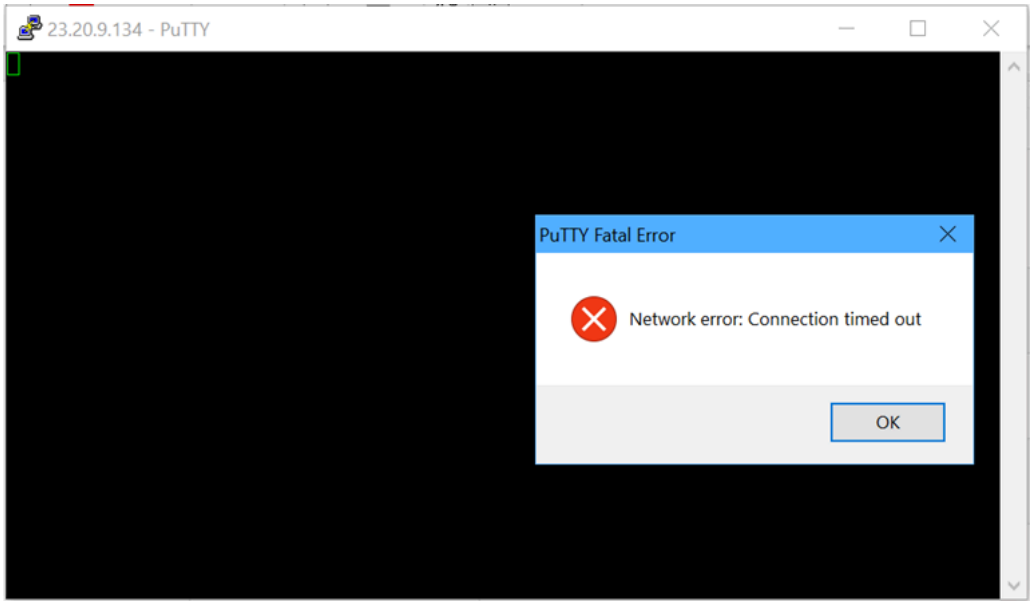


Рис. 3.28 – Термінал PuTTY після невдачі з'єднання

Успішне з'єднання без VPN, але невдача з VPN свідчить про правильність налаштувань безпеки для SSH.

Далі перевірте доступність вебсерверу до зовнішньої мережі. З'єднайтеся з вебсервером через PuTTY без VPN та протестуйте доступність за допомогою ping до зовнішньої IP-адреси, наприклад, 8.8.8.8, командою ping 8.8.8.8 (рис. 3.29).

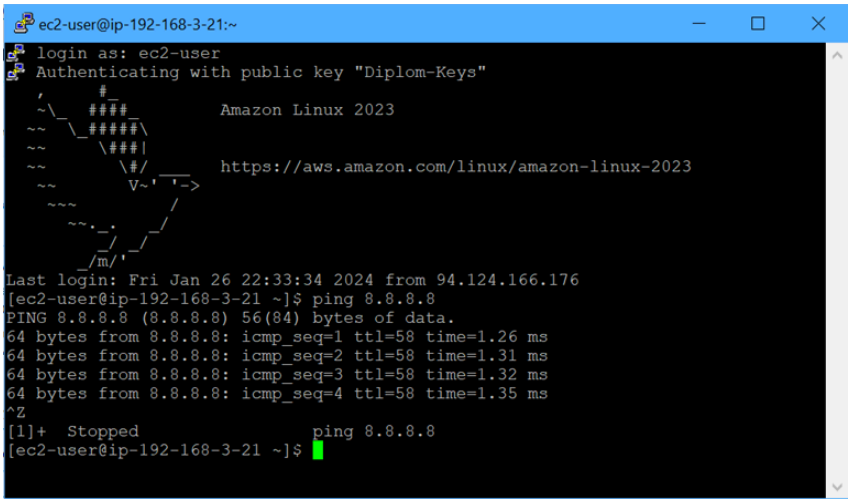


Рис. 3.29 – Тестування доступу до зовнішньої мережі

Наявність відповідей підтверджує доступність вебсервера до зовнішньої мережі. Далі перевірте можливість доступу до вебсервера зовнішньою мережею та коректність його налаштувань. Зробити це можна пошуком http://23.20.9.134/ в полі адресі веб-браузера. (рис. 3.30).

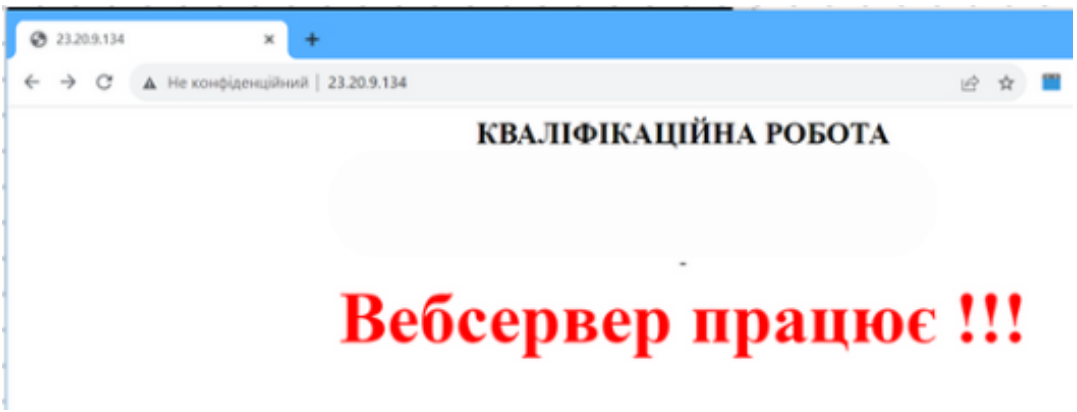


Рис. 3.30 – Тестова сторінка вебсерверу

Після введення адреси http://23.20.9.134/ у веб-браузері повинна з'явитися тестова сторінка, яка підтвердить доступність вебсервера та його правильні налаштування.

У разі успіху на всіх етапах тестування, правильність налаштувань груп безпеки, таблиць маршрутизації та загальної хмарної інфраструктури можна вважати підтвердженою.

Висновки за розділом 3

Розгортання хмарної інфраструктури AWS вимагає дотримання ряду необхідних параметрів, які включають у себе IP-адреси, налаштування приватних та загальнодоступних мереж, створення інтернет-шлюзів для забезпечення зв'язку з мережею Інтернет, а також налаштування безпеки за допомогою груп безпеки. Процес розгортання включає створення VPC, конфігурування підмереж, налаштування інтернет-шлюзів та інтерфейсів для шлюзів NAT, а також налаштування маршрутизаційних таблиць та груп безпеки для забезпечення безпеки серверів.

Цей розділ ілюструє процес створення та налаштування хмарної інфраструктури AWS, включаючи всі необхідні кроки для забезпечення безпеки та ефективності роботи. Враховуючи усі необхідні параметри та процеси, можна забезпечити стабільну та надійну інфраструктуру для розгортання різноманітних додатків та сервісів.

ВИСНОВКИ

У цій роботі було проведено детальний аналіз хмарної гібридної інформаційної системи, починаючи з огляду поняття хмарного сервісу, переваг і ризиків використання хмарної інфраструктури до вибору та розгортання платформи та технологій, зокрема з використання AWS.

Під час розгляду поняття хмарного сервісу були визначені базові терміни та переваги хмарної інфраструктури, а також вказані можливі ризики. У розділі "Огляд і вибір платформи та технологій" було проведено огляд передових хмарних платформ та технологій, з фокусом на AWS, і визначено їх можливості та функціонал.

Нарешті, у розділі "Розгортання хмарної інфраструктури AWS" було описано процес розгортання та налаштування інфраструктури AWS з урахуванням необхідних параметрів та заходів забезпечення безпеки.

Наукові завдання, вирішені в роботі, включають розуміння концепції та переваг хмарної інфраструктури, аналіз передових хмарних платформ та їх можливостей, а також навички розгортання та налаштування інфраструктури в AWS.

Проблеми, які можуть бути подальшим об'єктом досліджень, включають удосконалення заходів безпеки в хмарних сервісах, оптимізацію розгортання інфраструктури для підвищення ефективності та зменшення витрат, а також розробку нових методів моніторингу та управління ресурсами в хмарних сервісах.

У цілому, дана робота сприяє розумінню та впровадженню хмарної інфраструктури в сучасній інформаційній системі, а також вказує на напрями подальших досліджень у цій області.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Amazon Web Services — Вікіпедія [Електронний ресурс]. – режим доступу: URL: https://uk.wikipedia.org/wiki/Amazon_Web_Services (дата звернення – 23.05.2024).
2. Cloud Computing: Concepts, Technology & Architecture. Erl, Thomas, Puttini, Ricardo, Mahmood, Zaigham. C. 9-15.
3. Cisco Data Center Fundamentals. Maloo, Somit, Nikolov, Iskren. C. 33-37.
4. Data Center Handbook. 2nd Edition. Geng, Hwaiyu. C. 12-18.
5. Designing and Building a Hybrid Cloud. Trautman, Philip. C. 14-19.
6. GigaCloud — Вікіпедія [Електронний ресурс]. – режим доступу: URL: https://uk.wikipedia.org/wiki/GigaCloud (дата звернення – 23.05.2024).
7. Гібридна хмара: чим корисна для бізнесу та які задачі виконує | Kyivstar Business Hub [Електронний ресурс]. – режим доступу: URL: https://hub.kyivstar.ua/articles/gibrydna-hmara-chym-korysna-dlya-biznesu-ta-yaki-zadachi-vykonuye (дата звернення – 23.05.2024).
8. Google Cloud Platform — Вікіпедія [Електронний ресурс]. – режим доступу: URL: https://uk.wikipedia.org/wiki/Google_Cloud_Platform (дата звернення – 23.05.2024).
9. Habiba, Mansura. Hybrid Cloud Infrastructure and Operations Explained. C. 5-11.
10. Hybrid Cloud for Architects. Shrivastwa, Alok. C. 25-29.
11. Microsoft Azure — Вікіпедія [Електронний ресурс]. – режим доступу: URL: https://uk.wikipedia.org/wiki/Microsoft_Azure (дата звернення – 23.05.2024).
12. Найкращі хмарні сервіси України у 2022 році: дослідження Molfar – Molfar [Електронний ресурс]. – режим доступу: URL: https://molfar.com/blog/best-cloud-services-ukraine-2022 (дата звернення – 23.05.2024).

13. Хмарні сервіси зберігання даних - найкращі в Україні, надійні, ціна (tucha.ua) [Електронний ресурс]. – режим доступу: URL: https://tucha.ua/uk (дата звернення – 23.05.2024).

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В. Н. Каразіна

Факультет комп'ютерних наук
Кафедра теоретичної та прикладної системотехніки
Рівень вищої освіти (освітньо-кваліфікаційний рівень) **бакалавр**
Галузь знань: **12 – Інформаційні технології**
Спеціальність: **123 – Комп'ютерна інженерія.**

ЗАТВЕРДЖУЮ
Завідувач кафедри теоретичної
та прикладної системотехніки
д.т.н., проф. Шматков С. І.
«21» грудня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

КОНЮШЕНКО ПОЛІНИ ВІКТОРІВНИ

1. Тема роботи **«Мережна інфраструктура гібридної хмарної інформаційної системи»**
керівник роботи Агеєв Дмитро Володимирович професор, д.т.н.
затверджені наказом по університету від «03» травня 2024року № 4101-5/909

2.Строк подання студентом роботи 31 травня 2024року

3. Перелік питань, які потрібно розробити

1) Огляд існуючих моделей хмарних інформаційних систем.
2) Аналіз принципів побудови гібридних хмарних інформаційних систем.
3) Огляд та вибір платформи для створення гібридної хмарної інформаційної системи.
4) Огляд та вибір технологій і інструментів створення гібридної хмарної інформаційної системи.
5) Огляд принципів побудови та технологій розгортання мережної інфраструктури гібридної хмарної інформаційної системи.
6) Проектування архітектури гібридної хмарної інформаційної системи.
7) Розробка та реалізація прототипу мережної інфраструктури гібридної хмарної інформаційної системи.
8) Тестування та оцінка реалізованого прототипу, порівняння результатів з очікуваними показниками та аналіз отриманих висновків.
9) Оформлення пояснювальної записки.

4. План роботи

№ з/п	Назви етапів роботи	Термін виконання етапів роботи
1	Огляд існуючих моделей хмарних інформаційних систем.	21.12.2023 – 05.01.2024
2	Аналіз принципів побудови гібридних хмарних інформаційних систем.	14.02.2024 - 28.02.2024
3	Огляд та вибір платформи для створення гібридної хмарної інформаційної системи.	29.02.2024 - 15.03.2024
4	Огляд та вибір технологій і інструментів створення гібридної хмарної інформаційної системи.	1.03.2024 - 15.03.2024
5	Огляд принципів побудови та технологій розгортання мережної інфраструктури гібридної хмарної інформаційної системи.	1.03.2024 - 15.03.2024
6	Проектування архітектури гібридної хмарної інформаційної системи.	15.03.2024 - 15.04.2024
7	Розробка та реалізація прототипу мережної інфраструктури гібридної хмарної інформаційної системи.	20.03.2024 - 15.04.2024
8	Тестування та оцінка реалізованого прототипу, порівняння результатів з очікуваними показниками та аналіз отриманих висновків.	25.03.2024 - 30.04.2024
9	Оформлення звіту за результатами переддипломної практики.	15.05.2024 – 31.05.2024
10	Представлення кваліфікаційної роботи керівнику та рецензенту.	31.05.2024
11	Оформлення пояснювальної записки та підготовка презентації.	31.05.2024

5. Дата видачі завдання 21.12.2023

Студент П. В. Конюшенко
ініціали, прізвище
підпис

Керівник роботи Д. В. Агеєв
ініціали, прізвище
підпис

Додаток Б

Затверджую

_____

«_____»_____2024 р.

Технічне завдання

на розробку прототипу «Мережна інфраструктура гібридної хмарної інформаційної системи».

1.	Введення	1.1 Назва роботи – Мережна інфраструктура гібридної хмарної інформаційної системи. 1.2. Галузь застосування: Інформаційні технології
2.	Підстава для розробки	2.1. Навчальний план за спеціальністю 123 – Комп’ютерна інженерія 2.2. Завдання на кваліфікаційну роботу бакалавра № 4101-5/909 від «03» травня 2024 року (представити як Додаток А до пояснювальної записки до кваліфікаційної роботи).
3.	Призначення розробки	3.1. Мета розробки: Створення гібридної мережі в AWS для оптимізації та підвищення ефективності інфраструктури, яка об'єднує хмарні та локальні ресурси. 3.2. Призначення розробки: Забезпечення можливості ефективного використання ресурсів хмарної інфраструктури для розвитку, розгортання та управління додатками та послугами, а також для забезпечення безпеки, масштабованості та доступності системи. 3.3. Вхідні дані: Вхідними даними є вимоги до інфраструктури, обсяг трафіку, типи додатків та

		сервісів, які потрібно розгорнути в хмарному середовищі. 3.4. Вихідні дані розробки: Результатом розробки є гібридна мережа в AWS, яка надає надійне, масштабоване та безпечне середовище для розгортання додатків і послуг.
4.	Технічні вимоги до програмного виробу	4.1. Функціональні вимоги: - Здатність підключатися до різних типів хмарних інфраструктур та внутрішньої мережі - Забезпечення безпеки даних та мережі через використання різних методів аутентифікації та шифрування. 4.2. Нефункціональні вимоги: - Висока доступність системи, щоб забезпечити безперебійну роботу. - Висока продуктивність системи з можливістю ефективної обробки великих обсягів даних. - Простота в управлінні та налаштуванні для забезпечення легкості використання та підтримки. 4.3. Вимоги до інтеграції: - Можливість інтеграції з існуючими системами та платформами. - Сумісність з різними типами пристроїв та операційних систем. - Вимоги до відмовостійкості: - Здатність виявляти та виправляти помилки автоматично або шляхом сповіщень адміністратора. - Забезпечення резервного копіювання та відновлення даних. 4.4. Вимоги до безпеки:

		- Захист від зловмисних атак та витоку даних. - Забезпечення конфіденційності, цілісності та доступності інформації. - Вимоги до моніторингу та звітності: - Можливість моніторингу стану системи та її ефективності. - Наявність звітів про використання ресурсів та витрати.
5.	Вимоги до програмної документації	Документацією до виробу «Мережна інфраструктура гібридної хмарної інформаційної системи» вважати: 1) Опис основних вимог та функціональності системи (представити в розділі 4 пояснювальної записки до кваліфікаційної роботи). 2) Програму і методику випробувань розробленої програми (представити як додаток В до пояснювальної записки до кваліфікаційної роботи). 3) Опис розробленого прототипу мережі (представити в розділі 3 пояснювальної записки до кваліфікаційної роботи).
6.	Вимоги до техніко-економічних показників	Документацією до виробу «Мережна інфраструктура гібридної хмарної інформаційної системи» вважати: 1) Справжнє Технічне завдання на розробку прототипу мережі (представити у вигляді Додатку Б до пояснювальної записки до кваліфікаційної роботи). 2) Опис розробленого прототипу мережі (представити в розділі 3 пояснювальної записки до кваліфікаційної роботи). 3) Джерела базової інформації.

	Етапи роботи	Дата та назва	
		14.02.2024 - 28.02.2024	Огляд існуючих моделей хмарних інформаційних систем.
		14.02.2024 - 28.02.2024	Аналіз принципів побудови гібридних хмарних інформаційних систем.
		29.02.2024 - 15.03.2024	Огляд та вибір платформи для створення гібридної хмарної інформаційної системи.
		1.03.2024 - 15.03.2024	Огляд та вибір технологій і інструментів створення гібридної хмарної інформаційної системи.
		1.03.2024 - 15.03.2024	Огляд принципів побудови та технологій розгортання мережної інфраструктури гібридної хмарної інформаційної системи.
		15.03.2024 - 15.04.2024	Проектування архітектури гібридної хмарної інформаційної системи.
		20.03.2024 - 15.04.2024	Розробка та реалізація прототипу мережної інфраструктури гібридної хмарної інформаційної системи.
		25.03.2024 - 30.04.2024	Тестування та оцінка реалізованого прототипу, порівняння результатів з очікуваними показниками та аналіз отриманих висновків.
		15.05.2024 – 31.05.2024	Оформлення звіту за результатами переддипломної практики.
		31.05.2024	

		31.05.2024	Представлення кваліфікаційної роботи керівнику та рецензенту. Оформлення пояснювальної записки та підготовка презентації.
8.	Порядок контролю і приймання програмного продукту (моделі)	1. Перевірку ходу розробки прототипу мережі виконувати раз в 3 тижні. 2. Захист розробленої моделі провести на засіданні Атестаційної комісії. 3. Пояснювальну записку подати на паперових носіях в 1 примірнику.	

Виконавець

Студентка групи КІ-41

Конюшенко П. В.

_____

Замовник

д. техн. наук, проф.

Агеєв Д. В.

_____

Додаток В

Програма і методика випробувань програмного виробу

«Мережна інфраструктура гібридної хмарної інформаційної системи»

1. Об’єкт випробувань

1. Назва розробленого прототипу: «Мережна інфраструктура гібридної хмарної інформаційної системи».

2. Галузь застосування: Інформаційні системи

3. Перераховані відомості запозичуються з відповідних розділів Технічного завдання.

2. Мета випробувань

Перевірка відповідності функціональні можливості системи заявленим функціональним можливостям в технічному завданні (Додаток Б до пояснювальної записки до кваліфікаційної роботи).

3. Загальні положення

1. Підстави для проведення випробувань

Підставою для проведення випробувань є наказ про призначення атестаційної комісії.

2. Місце і тривалість випробувань

Приймальні (приймально-здавальні) випробування проводяться на базі комп’ютерного класу кафедри в період роботи атестаційної комісії.

3. Обсяг випробувань

Приймальні випробування програмного виробу проводяться в обсязі відповідному цієї програми і методики випробувань.

4. Організації, які беруть участь у випробуваннях

Приймальні випробування проводяться атестаційною комісією напередодні засідання (або в процесі засідання) за участю Замовника, Виконавці та інших осіб, присутніх на засіданні.

4. Вимоги до програми або програмного виробу

4.1. Функціональні вимоги:

- Здатність підключатися до різних типів хмарних інфраструктур та внутрішньої мережі
- Забезпечення безпеки даних та мережі через використання різних методів аутентифікації та шифрування.

4.2. Нефункціональні вимоги:

- Висока доступність системи, щоб забезпечити безперебійну роботу.
- Висока продуктивність системи з можливістю ефективної обробки великих обсягів даних.
- Простота в управлінні та налаштуванні для забезпечення легкості використання та підтримки.

4.3. Вимоги до інтеграції:

- Можливість інтеграції з існуючими системами та платформами.
- Сумісність з різними типами пристроїв та операційних систем.
- Вимоги до відмовостійкості:
- Здатність виявляти та виправляти помилки автоматично або шляхом сповіщень адміністратора.
- Забезпечення резервного копіювання та відновлення даних.

4.4. Вимоги до безпеки:

- Захист від зловмисних атак та витоку даних.
- Забезпечення конфіденційності, цілісності та доступності інформації.
- Вимоги до моніторингу та звітності:
- Можливість моніторингу стану системи та її ефективності.
- Наявність звітів про використання ресурсів та витрати.

5. Вимоги до програмної документації

Програмною документацією до прототипу мережі «Мережна інфраструктура гібридної хмарної інформаційної системи» вважати:

1) Справжнє Технічне завдання на розробку прототипу мережі (представити у вигляді Додатку Б до пояснювальної записки до кваліфікаційної роботи).

2) Опис реалізованого прототипу мережі (представити в розділі 3 пояснювальної записки до кваліфікаційної роботи).

3) Джерела базової інформації.

6. Засоби і порядок випробувань

6.1. Засоби випробувань

Засоби випробувань представлено на ПК на яких встановлено наступні програмні засоби: Браузер.

6.2. Порядок проведення випробувань

Як правило, випробування проводяться в два етапи:

- Ознайомчий (1-й етап);
- Власне випробування програмного виробу (2-й етап).

Перелік перевірок, що проводяться на 1 етапі випробувань, включає в себе:

1) Перевірку комплектності складу програмної документації здійснюються за критерієм наявності зазначеної в ТЗ документації

2) Перевірка якості документації. Перевірку здійснювати за критерієм відповідності вимогам ГОСТ 34.602-89 "Автоматизовані системи. Система стандартів на автоматизовані системи. Зміст і структура технічного завдання"

Методика проведення перевірок:

Для початку треба запустити AWS Console та увійти до облікового запису.

1. Знайдіть публічну IP-адресу вебсервера в консолі «Amazon EC2» у полі «Public IPv4 address» – це 23.20.9.134.
2. Перевірте IP-адресу за допомогою ресурсу https://myip.ms/. Порівняйте її з IP-адресою у налаштуваннях групи безпеки вебсервера.
3. Під'єднайтесь до вебсервера через SSH за допомогою PuTTY:

- виберіть ключ Diplom-Keys.ppk у панелі автентифікації;

- вкажіть публічну адресу 23.20.9.134;
- після успішного з'єднання введіть логін ec2-user і завершіть з'єднання командою exit.

4. Для перевірки доступності вебсервера з іншої IP-адреси:
- підключіться до VPN;
- перевірте IP-адресу за допомогою ресурсу https://myip.ms/;
- спробуйте з'єднатися з вебсервером через SSH. З'єднання має бути невдалим.

5. Перевірте доступність вебсервера до зовнішньої мережі:
- під'єднайтесь до вебсервера через PuTTY без VPN;
- Виконайте команду ping 8.8.8.8. Наявність відповідей підтвердить підключення.

6. Перевірте можливість доступу до вебсервера через браузер:
- введіть адресу http://23.20.9.134/. Тестова сторінка підтвердить правильність налаштувань.

7. Перевірте доступ вебсервера до сервера баз даних:
- введіть адресу http://23.20.9.134/SamplePage.php. З'явлення інформації з сервера баз даних і можливість додати новий запис підтвердять правильність налаштувань.

Успішне виконання всіх тестів підтвердить правильність налаштувань безпеки, таблиць маршрутизації та хмарної інфраструктури.

Виконавиця: студентка групи КІ-41, Конюшенко П.В.