Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра

на тему: «Методи та технології побудови захищеної хмарної інфраструктури для інтернет-магазину на Amazon Web Services»

Виконала студентка 2-го курсу групи КБм-22-1
спеціальності 125 «Кібербезпека»
Д.Р. Кручинська

Керівник завідувач кафедри комп'ютерної інженерії та кібербезпеки, кандидат технічних наук, доцент
А.А. Єфіменко

Рецензент доцент кафедри комп'ютерної інженерії та кібербезпеки, кандидат технічних наук, доцент
Ю.М. Россінський

Житомир – 2023

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

Андрій Єфіменко

13 жовтня 2023 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу магістра

Студентки: Кручинської Дар'ї Романівни

Тема роботи: «**Методи та технології побудови захищеної хмарної інфраструктури для інтернет-магазину на Amazon Web Services**»

затверджена Наказом університету від 13 жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи 11 грудня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Наукові джерела з питань хмарних послуг.
2. Нормативно-правові джерела щодо хмарних технологій.
3. Документація Amazon Web Services.

Обладнання та програмне забезпечення:

1. Amazon Web Services.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	В.В. Воротніков	13.10.23	13.10.23
2	В.В. Воротніков	30.10.23	30.10.23
3	В.В. Воротніков	20.11.23	20.11.23

Студентка _____ Д.Р. Кручинська

Керівник _____ А.А. Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	13 жовтня 2023	
2	Пошук, огляд та аналіз аналогічних розробок	14 жовтня 2023 – 15 жовтня 2023	
3	Опрацювання літературних джерел	16 жовтня 2023	
4	Аналіз моделей, типів та принципів застосування хмарних технологій	17 жовтня 2023 – 22 жовтня 2023	
5	Створення акаунту в системі AWS та аналіз усіх існуючих сервісів даної системи	23 жовтня 2023 – 29 жовтня 2023	
6	Розробка архітектури хмарного сервісу та UML – моделі	30 жовтня 2023 – 3 листопада 2023	
7	Реалізація аутентифікації клієнтів та методів доступу до веб-додатку	4 листопада 2023 – 10 листопада 2023	
8	Розгортання клієнтської та серверної частин хмарної інфраструктури	11 листопада 2023 – 21 листопада 2023	
9	Налаштування сервісів захисту та розгортання комерційної частини інфраструктури	22 листопада 2023 – 27 листопада 2023	
10	Аналіз отриманих результатів	28 листопада 2023	
11	Формування пояснювальної записки	29 листопада 2023 – 6 грудня 2023	
12	Підготовка презентації та виступу	7 грудня 2023	
13	Отримання відгуку від керівника та рецензії на кваліфікаційну роботу		
14	Захист		

Студентка _____ Д.Р. Кручинська

Керівник _____ А.А. Єфіменко

РЕФЕРАТ

Випускна кваліфікаційна робота магістра складається з проєкту захищеної архітектури хмарної інфраструктури та пояснювальної записки. Пояснювальна записка до випускної роботи викладена на 114 сторінках, містить 99 рисунків, які розміщено на 60 сторінках. Перелік джерел посилань містить 26 літературних джерел і займає 3 сторінки.

Метою роботи є спрощення та налаштування безпеки як внутрішньої, так і зовнішньої для користувачів. І важливим елементом є спрощення та автоматизація у роботі для співробітників. Всі ці моменти будуть реалізовуватись за допомогою хмарних технологій на базі Amazon Web Services.

Об'єктом дослідження є процес проєктування захищеної хмарної інфраструктури.

Предметом дослідження є архітектура, елементи захисту інформації, класифікація та методи проєктування хмарної інфраструктури.

У першому розділі кваліфікаційної роботи представлено огляд сучасних технологій хмарних обчислень з описом моделей та типів хмарних обчислень, проведено аналіз плюсів та мінусів хмарної інфраструктури у різних сферах використання. Другий розділ демонструє створення акаунту у системі AWS та докладний аналіз сервісів AWS і їх принципи функціонування, також вміщено розробку архітектури хмарної інфраструктури для інтернет-магазину з підбором сервісів та розроблена UML-діаграма прецедентів. Третій розділ присвячений реалізації архітектури хмарної інфраструктури на практиці. Перевірка працездатності реалізованої хмарної інфраструктури здійснена за допомогою сервісу AWS. Проєкт працездатний та готовий до впровадження. Перспективний є розробка конкретного веб-додатку інтернет магазину для інтеграції його зі створеною хмарною інфраструктурою.

Ключові слова: ХМАРНА ІНФРАСТРУКТУРА, ХМАРА, АРХІТЕКТУРА, ІНТЕРНЕТ-МАГАЗИН.

ABSTRACT

The final qualification work of the master consists of a project of a secure cloud infrastructure architecture and an explanatory note. The explanatory note to the qualification work is laid out on 114 pages, contains 99 figures, which are placed on 60 pages. The list of reference sources contains 26 literary sources and occupies 3 pages.

The purpose of the work is to simplify and configure both internal and external security for users. And an important element is the simplification and automation of work for employees. All these points will be implemented using cloud technologies based on Amazon Web Services.

The object of research is cloud infrastructure design technology.

The subject of research is architecture, information protection elements, classification and methods of cloud infrastructure design.

The first chapter of the qualification work presents an overview of modern cloud computing technologies with a description of cloud computing models and types, an analysis of the pros and cons of cloud infrastructure in various areas of use. The second section demonstrates the creation of an account in the AWS system and a detailed analysis of AWS services and their principles of operation, also contains the development of the cloud infrastructure architecture for an online store with a selection of services and a developed UML diagram of precedents. The third section is devoted to the implementation of cloud infrastructure architecture in practice. The performance check of the implemented cloud infrastructure was carried out using the AWS service. The project is operational and ready for implementation. The development of a specific web application of an online store for its integration with the created cloud infrastructure is promising.

Keywords: CLOUD INFRASTRUCTURE, CLOUD, ARCHITECTURE, INTERNET STORE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AWS	–	Amazon Web Services
SaaS	–	Software as a Service
PaaS	–	Platform as a Service
IaaS	–	Infrastructure as a Service
NIST	–	National Institute of Standards and Technology
SMAC	–	Social Mobile Analytics Clouds
API	–	Application Programming Interface
VPC	–	Virtual Private Cloud
AI	–	Artificial intelligence
SAN	–	Storage Area Network
NAS	–	Network-attached Storage
IoT	–	Internet of Things
DevOps	–	Development & operations
B2C	–	Busibess-to-Consumer
MFA	–	Multi-factor authentication
ACL	–	Access Control List
DNS	–	Domain Name System
ЦОД	–	Центр обробки даних
ЗВО	–	Заклад вищої освіти
БД	–	Бази даних
СУБД	–	Система управління базами даних

ВСТУП

З розвитком нових технологій та в загальному Інтернету, виникає потреба у нових можливостях для компаній, підприємств, різних державних та не державних установ тощо. Постає завжди питання спрощення використання тих чи інших можливостей, а головне забезпечення безпеки даних, як комерційного, так і особистого характеру.

В умовах сьогодення, на прикладі нашої держави, а саме повномасштабної війни, наслідки всесвітньої пандемії та інші менш вагомі труднощі, вимушено перемістили у дистанційну форму роботи, навчання тощо, досить велику кількість компаній, деякі державні установи, навчальні заклади і т.д. Але навіть ті компанії, які не працюють в онлайновій формі, задумались про нові зміни, можливості та забезпечення себе високопродуктивними технологіями.

Саме така технологія є «хмара», також відома як «хмарні технології» або ж «хмарні обчислення». Це не нова технологія, вона існує вже досить значний час, зокрема в інших частинах світу хмарні технології використовуються вже у багатьох компаніях, установах і їх використання показало вже досить багато плюсів, як для компаній та і для користувачів.

В Україні, впровадження хмарних технологій на підприємствах тощо., тільки починає набирати популярності, але я думаю, що найближчим часом досить значна частина як великих, так і малих підприємств зробить цей перехід. Наприклад, навесні цього року, було підписано закон в Україні про хмарні послуги, що супроводжується перенесенням даних державних органів у хмарні середовища [2]. І це тільки початок, також було врегульоване питання використання банками хмарних технологій, з метою забезпечення банками оброблення та зберігання інформації про банківські операції, а також захисту персональних даних клієнтів банків в умовах воєнного стану, протягом воєнного стану та впродовж двох років після його скасування [3].

Оскільки нарешті державні установи, банки та навіть деякі компанії вже впроваджують, або ж впровадили хмарні технології, то більшість компаній як великих, так і малих зробить цей крок до нових можливостей.

Хмарна інфраструктура в свою чергу є економічною, що дозволяє заощаджувати бюджет, є можливість масштабування хмари у випадку збільшення інтернет – магазину, або ж відмови на деякий час від серверів, якими не користуються. Відповідно від навантаження та потреб, можна оптимально організувати власну хмарну інфраструктуру з перспективою повної міграції всього бізнесу в хмару.

Завдання, які вирішує хмарна інфраструктура, мають досить вагомий внесок в покращення та полегшення бізнес-процесів. Одним з найголовніших завдань, які вирішує інфраструктура у хмарі, є пришвидшений процес отримання обчислювальних ресурсів чи даних, які необхідні вже зараз. За допомогою різновиду інструментів для автоматизації, виділення ресурсів хмари для кінцевого користувача стає значно швидшим, що ефективно впливає на бізнес.

Другим завданням, яке вирішує хмарна інфраструктура, варто зазначити зниження навантаження на персонал, який керує інфраструктурою та додатками у хмарі. Адже завдяки інструментам які надаються для автоматизації, скорочується час на розгортання віртуальних серверів та внутрішніх складових інфраструктури, що в подальшому додає час для працівників у роботі з внутрішніми та зовнішніми проєктами які розвивають саму інфраструктуру для бізнесу.

І найголовнішим завданням є підвищення безпеки як всієї інфраструктури, так і конфіденційної інформації. З огляду широкого асортименту політик безпеки, які пропонуються для хмарних інфраструктур, які безпосередньо мають централізоване керування, що дає змогу значно швидше та легше здійснювати контроль вже існуючих політик, та звичайно впроваджувати нові. Безпека даних завжди залишається одним з найголовніших завдань, які повинна вирішувати та чи інша технологія.

Звичайно, що це не весь діапазон завдань, які допомагає вирішити хмарна інфраструктура, але це основні та найважливіші. В залежності від специфіки інтернет – магазину та побудованої хмарної інфраструктури для такого бізнесу, можна гнучко визначати завдання різного типу, саме під потребу замовника. Це є вагомою перевагою, і не тільки для бізнесу.

Актуальність роботи полягає в тому, що проєкт хмарної інфраструктури, який буде спроєктовано під інтернет-магазин, можна буде з легкістю адаптувати під різні сфери торгівлі, що є досить ефективною практикою.

Метою цього проєкту є спрощення та налаштування безпеки як внутрішньої, так і зовнішньої для користувачів. Також важливим елементом є полегшення та автоматизація роботи для співробітників. Всі ці моменти будуть реалізовуватись за допомогою хмарних технологій на базі Amazon Web Services.

Об'єктом дослідження є процес проєктування захищеної хмарної інфраструктури.

Предметом дослідження є архітектура, елементи захисту інформації, класифікація та методи проєктування хмарної інфраструктури.

Для досягнення зазначеної мети необхідним є вирішення наступних взаємозалежних науково-технічних задач:

- провести аналіз та узагальнення моделей та типів хмарних сервісів;

- провести аналіз сфер застосування хмарних технологій та визначити переваги та недоліки;

- визначити класифікації та принципи функціонування базових веб-сервісів в системі AWS;

- провести аналіз елементів захисту інформації притаманні системі AWS;

- розробити архітектуру інфраструктури хмарного сервісу;

- провести реалізацію інфраструктури хмарного сервісу;

Наукова новизна отриманих результатів полягає в тому, що під час дослідження, уточнено та розглянуто нові факти у хмарних технологіях в

результаті яких спроєктовано та реалізовано універсальну хмарну інфраструктуру для інтернет-магазину.

Практичне значення одержаного результату має надзвичайно вагомий внесок та спрощення для багатьох компаній, адже спроєктовану модель можна з легкістю адаптувати під різні галузі та масштаби бізнесу, в яких потрібно інтернет - магазин. Що в свою чергу дозволяє спрощену форму міграції вже існуючих інтернет – магазинів у хмару.

РОЗДІЛ 1. Аналіз принципів, моделей та технологій хмарних сервісів

1.1 Поняття «хмарні технології»

У епоху нових технологій та можливостей, в різних сферах відбувається впровадження чогось нового або ж розвиток та популяризація того, що вже було. Хмарні технології не стали винятком у списку популярних технологій та інновацій на сьогодні.

Існує безліч літератури, статей та тез, як і думок спеціалістів з приводу саме термінології та понять. При дослідженні поняття одразу виникає питання «хмарні технології» чи «хмарні обчислення». В чому ж різниця, чи все ж таки це одне й те саме. І багато різних інших питань пов’язаних саме з термінами. В принципі скільки людей, стільки ж думок. Тому логічно, що кожен визначає поняття та термінологію зі своєї точки зору та свого особистого досвіду.

Ситуація з термінологією також погіршується, тому що різні хмарні провайдери, аналогічно як і експерти в цій галузі, дають свої визначення різним поняттям у хмарній сфері. Саме тому завжди потрібно проводити аналіз самостійно, аби віднайти ту саму істину, адже у термінології завжди є спірні питання.Аналізуючи різні терміни, думки експертів та науковців у даній сфері та головне проводячи своє дослідження з аналізу впровадження хмарних технологій у різних компаніях як за кордоном, так і в нашій країні, можна зробити висновки.

Хмарні технології надають готові рішення замовникам та користувачам, тобто це готові рішення, які можна використовувати в тій чи іншій установі. Однією із вимог використання таких рішень, є наявність будь-якого пристрою, який має можливість під’єднання до глобальної мережі Інтернет. Ця вимога є однією з основних тому, що при підключенні до всесвітньої мережі Інтернет, користувач зможе отримати доступ до бази даних, яка буде знаходитись на віддаленому сервері.

Хмарні технології – це технологія обробки даних, за допомогою яких надаються комп'ютерні ресурси у всесвітній мережі Інтернет, як онлайн сервіс, відповідно до вимог користувача. Тобто іншими словами, хмарні технології, це як одна велика концепція, яка містить в собі велику кількість різних ресурсів, які надають послуги.

Також при вивченні понять хмарних технологій, необхідно звернути увагу на таке поняття, як хмарний сервіс. Хмарний сервіс являє собою послугу надання хмарних ресурсів для користувача за допомогою такої технології, як «хмарні обчислення». [4]

Хмарні обчислення (англ. cloud computing) або скорочено «хмара» – це модель, яка забезпечує всюди зручний доступ мережею, на вимогу, до спільного пулу обчислювальних ресурсів, таких як сервери, програми, служби, бази даних тощо, які можуть бути оперативно надані на вимогу та аналогічно звільнені з мінімальними зусиллями управління, або взаємодії постачальника послуг.[5] Термін «хмара» (cloud) використовується як метафора, яка заснована на схемі комп'ютерної мережі, або як образ складної інфраструктури, за якою ховаються всі технічні моменти.[6]

1.2 Актуальність використання хмарних технологій

Використання хмарних технологій вже показали гарні результати у різних країнах, адже дана технологія вже досить значний час використовується у різних країнах та різних сферах життя. Звичайно час не стоїть на місці, тому розвиток хмари все більше набирає свої оберти та це стосується не тільки інших країн, але й України. Попри те, що використання хмарних технологій в Україну прийшло зі значним запізненням, за останні роки було зроблено низку вагомих кроків у розвитку даної технології в Україні.

Зокрема, за останні роки хмарні технології стали популярними не тільки у пересічного користувача в особистих інтересах, але й у бізнесі. Низка компаній або вже зробила міграцію у хмару, або ж знаходиться тільки на етапі міграції, або ж планує у майбутньому мігрувати у хмару. І звичайно рішення

про міграцію у хмару не обходить і державні установи та звичайно сферу освіти, адже це допомагає рухатись у напрямку Євроінтеграції.

Розвиток інновацій не стоїть на місці, технології розвиваються кожен день, тому звичайно це все спонукає до пошуку нових можливостей, аби встигати за прогресом і не тільки. Підвищення інтересу до міграції у хмару спричиняє також і низка проблем яка виникає, через воєнний стан у нашій країні.

Після початку повномасштабної війни проти України у багатьох організаціях постало питання не тільки зберігання, а й не втрати даних, з огляду кібербезпеки, адже резервне збереження даних має бути захищеним. Звичайно вирішення такої низки питань в перше чергу вимагає швидкого реагування та якнайшвидшого розв'язання питання. Також на це потрібні немалі обсяги обчислювальних ресурсів, а це все витрати. Саме тому на допомогу розв'язання таких питань і прийшли хмарні технології, які економлять час організації роботи, безпеку, економію ресурсів та пропонування власних обчислювальних елементів за потреби.

Як результат низки таких рішень вже видно зростання попиту на використання саме хмарних сервісів. Одним з таких прикладів є міграція в хмару одного з найбільших банків України, а саме 270 сервісів ПриватБанку та понад 4 петабайти клієнтської інформації. [7] Звичайно, що на цьому міграція не закінчена, але найголовніше, що початок вже покладений. Це не єдиний приклад міграції банку у хмару в Україні й звичайно, що попит буде тільки збільшуватись.

Важливим фактором є те, що наша країна з початком повномасштабної війни, отримала величезну підтримку та допомогу від таких компаній як Amazon, Google та Microsoft, які є лідерами у хмарних технологіях та найголовнішими постачальниками хмарних послуг і додатково від інших, саме для підтримки нашого бізнесу, держави та звичайно IT – сфери. Тому це пришвидшило міграцію десятків тисяч проєктів, систем та компаній у публічну хмару і не тільки. [8]

Галузь бізнесу і не тільки, завжди розглядає нові рішення оптимізації через те, що масштаби продовжують рости, саме тому найпоширенішим способом перенесень навантажень були хмарні технології, або ж ЦОД (центр обробки даних). Кожен звичайно обирав той варіант, який більш підходить до його запитів. Але знову ж в умовах війни все змінилось, і зараз через ризики обстрілів та влучань у наземні ЦОД та відключення електропостачання, перевагу надають міграції у хмару. Звичайно з закінченням війни все може змінитись, але наразі хмара залишається надійнішим та безпечнішим варіантом для зберігання даних та безперебійності роботи. [7]

Одним з факторів популярності використання хмарних технологій саме в Україні є те, що вже існують українські провайдери які пропонують свої послуги для вітчизняного ринку і не тільки. Зокрема з дослідження компанії Molfar, у якому визначали найкращий хмарний сервіс України, взяли участь 17 провайдерів України. Досліджувалась різна інформація, яка стосувались обслуговування, особливостей співпраці, тарифи та звичайно використання самих сервісів зсередини. Перше місце у досліджені зайняли дві компанії GigaCloud та Tetcloud. [9]

З огляду на розвиток технологій, хмарні сервіси будуть ставати тільки популярнішими, а найближчим часом не тільки великі компанії та корпорації зроблять перехід у хмару, але й маленькі підприємства. Найближчим часом частка конфіденційних даних, які зберігаються у хмарі буде тільки зростати та головне не тільки у світі, але й в Україні.

1.3 Моделі хмарних сервісів

Технології не стоять на місці та постійно продовжують рухатись та вдосконалюватись. У світі існують різні моделі хмарних сервісів, які створені, як обчислювальні послуги. Іншими словами вони є віддаленими, і відрізняються відповідно до запитів клієнтів. У виборі моделі хмарного сервісу все залежить від потреб реалізації, наприклад функціональних можливостей, фінансових, запитів тощо.

З огляду найчастіших вподобань компаній при виборі моделі, можна виділити 3 найпопулярніші моделі, які надають світові провайдери:

1. Software as a Service (SaaS) – програмне забезпечення як послуга.

2. Platform as a Service (PaaS) – платформа як послуга.

3. Infrastructure as a Service (IaaS) – інфраструктура як послуга.

Представлені моделі є найпопулярнішими, та мають звичайно відмінності, які підходять тій чи іншій компанії. Зокрема ці три моделі також у своїх стандартах виділяє NIST [5]. Ці визначення публікуються для забезпечення узгодженості та компромісного рішення для застосування у всьому світі, але звичайно вони не виключають інші точки зору, які сформовані від потреб та географічних розташувань.[1]

Найпопулярнішою моделлю хмарних обчислень, яку обирає більшість підприємств та установ, з усіх представлених від хмарних провайдерів на ринку, все ж таки є програмне забезпечення як послуга (SaaS).

Модель програмного забезпечення як послуги (SaaS) являє собою готове рішення для користувача з мінімальною необхідністю налаштувань під заявлені потреби. Однією з переваг такої моделі є те, що обираючи саме її, керувати нею зможе будь-який користувач, якщо залучити мінімально до цього процесу, наприклад системного адміністратора, або ж навіть і без нього.

Тобто користувач має можливість використовувати різні додатки, які в цей час будуть розміщені у самій хмарі, але при цьому всьому не контролюючи власне інфраструктуру хмари, сховища зі збереженими даними та саму мережу серверів провайдера тощо. У свою чергу, користувач має можливість взаємодіяти з конфігурацією якогось конкретного додатка для користувачів. [10] Однією з переваг такої моделі є те, що все працює через веб-браузер, тому такий додаток доступний на будь-якому пристрою, та не залежно від того, яка операційна система налагоджена.

Наступна модель (PaaS) – платформа як послуга, яка являє собою онлайн – ресурси, та представляється у вигляді різних платформ з наборами інструментів та середовищами, які використовуються для розробки

програмного продукту, або ж використання вже наявних додатків, серверів тощо. [11]

Дану модель зазвичай обирають розробники, оскільки обравши саме цю модель, користувач контролює свої розгорнуті чи розроблені програми, що є зручним, але все ж керування базовою інфраструктурою, та ще деякими можливостями залишається недоступним.

Вагомим мінусом даної моделі є те, що вони гарно себе зарекомендували при використанні у великих корпораціях, але на жаль при використанні у малих підприємствах були виявлені недоліки та ефективність використання показала не найкращі результати.

Наступна модель хмарного сервісу відкрила нові можливості для розвитку компанії, мінімізуючи витрати та ресурси. Хмарна інфраструктура як послуга (IaaS) виступає аналогом вже існуючих апаратних засобів, таких як сховища, процесори тощо, лише віртуальна та розміщуючись опосередковано у хмарі.

Відповідно обираючи дану модель, користувач орендує потрібні йому ресурси, які є віртуальними та не потребують додаткових приміщень, або ж витрат, та встановлює на дані ресурси саме ті операційні системи чи програми які йому потрібно.

Звичайно, що дана модель не така популярна як інші серед звичайних користувачів, через свої особливості, але її полюблять системні адміністратори. У сучасних компаніях, хмарна модель (Iaas) досить гнучко масштабується, що дозволяє економити як витрати, так і ресурси, в залежності від потреб компанії на даний час. Це є однією з головних переваг даної моделі.

Звичайно існують і інші моделі хмарних сервісів, які продовжують вдосконалюватись та розвиватись кожен день, але все ж (Saas), (PaaS) та (Iaas) є найпопулярнішими на даний час. Звичайно вибір залишається за компанією яка хмарна модель підійде саме їм. Вибір повинен робитися випливаючи із потреб, та враховуючи, яку ж саме частину компанія готова віддати на аутсорсинг.

1.4 Типи хмарних обчислень

На даний час NIST та ISO/IEC виділяють чотири однакові типи хмарних обчислень: приватна хмара (Private Cloud), хмара співтовариства або загальна хмара (Community Cloud), публічна хмара (Public Cloud), гібридна хмара (Hybrid Cloud). [1]

Приватна хмара (Private Cloud) – це інфраструктура, яка виділяється тільки для використання лише однією організацією, яка у свою чергу, складається з декількох споживачів.

Такий тип хмарного обчислення може бути представлений у декількох варіантах, таких як перебування у власності, під управлінням та керуватись організацією, яка у свою чергу буде виступати у ролі третьої сторони. Також це може бути комбінацією представлених варіантів керування, яка буде підлаштована під самого замовника. В незалежності від управління приватною хмарою, вона може розташовуватись як на території, наприклад компанії, так і за її межами.

Хмара співтовариства або загальна хмара (Community Cloud) – тип хмарної інфраструктури, який надається для користування виключно певній спільноті споживачів з організацій, які пов’язані між собою спільними інтересами чи характеристиками (наприклад політика компанії, вимоги безпеки, рівні відповідальності тощо).

Даний тип хмари може бути власністю, який буде керуватись однією або декількома організаціями в установі, або ж третьою стороною, яка буде найманою компанією, в залежності від політики безпеки компанії.

Аналогічно до приватної хмари, така хмара може розташовуватись як в приміщені компанії, так і за її межами, та комбінувати в собі методи управління в залежності від вимог чи правил компанії тощо.

Публічна хмара (Public Cloud) – використовується у відкритому доступі та слугує інфраструктурою для широкого загалу.

Керувати публічною хмарою може як державна організація, так і комерційна, або ж це можна комбінувати. Даний вид хмар, як правило

розташовані на території хмарних провайдерів, які й надають різні види послуг.

Гібридна хмара (Hybrid Cloud) – представляє собою комбінацію двох або більше різних хмар інфраструктури (приватні, публічні, загальні або співтовариства), які у свою чергу залишаються унікальними, але пов’язані між собою за допомогою технологій (стандартизованих чи запатентованих), та дозволяють передавати дані та послуги між хмарами.[5]

1.5 Сфери застосування хмарних технологій

Вже зараз хмарні технології стали невід'ємною складовою у багатьох сферах життя, як в особистому розумінні, так і глобальному. Достатньо велика кількість компаній вже зберігає у хмарах не тільки дані, але й деякі відділи мігрують у хмару, а деякі компанії навіть повністю переносять свою інфраструктуру компанії у хмару. І звичайно це стосується не тільки бізнес сфери, але й більш соціальних сфер.

Можна виділити найпопулярніші сфери застосування хмарних технологій на сьогодні:

1. Керування бізнесом.

З огляду управління бізнесом з використанням хмарних технологій, кожна компанія обирає свою траєкторію напрямку та сценарій реалізації хмари у своїй компанії. Дане рішення випливає з потреб та завдань компанії, які є унікальними для кожної навіть в одному секторі бізнесу.

Для однієї компанії найголовнішим питанням буде власна безпека та безпека конфіденційної інформації клієнтів компанії. А для іншого підприємства буде найголовнішим питання заощадження коштів виділеного бюджету. Даний перелік може продовжуватись далі, та змінюватись від потреб та різних факторів.

Можна виділити ряд більш використовуваних сценаріїв використання хмарних технологій у бізнесі:

- **Сховище резервних копій.** Даний сценарій є найпопулярнішим та найпростішим і звичайно він також охоплює низку варіантів його використання:

- Резервні копії можна зберігати на віддаленому майданчику, для безпеки бекапів у випадку неполадок на головному майданчику.
- Зберігання даних в сертифікованому дата – центрі, для більшої захищеності даних, так як файли передаються захищеними каналами, а на самих дисках інформація буде захищатись апаратним шифруванням.

За необхідності є можливість відновлення даних із резервних копій на віддаленому майданчику, за умови домовленості з хмарним провайдером.

- **Резервний майданчик.** Використання хмарного рішення для організації резервного майданчика, як правило реалізовується задля відмови будування власного кластера, що у свою чергу, дозволяє зекономити як кошти, так і час на організацію відмовостійкої локальної інфраструктури. Резервний майданчик виступає для безперебійності роботи у разі, якщо основна інфраструктура вийде з ладу, або ж дасть збій, робота продовжиться на резервному майданчику. Цей варіант підходить не тільки для маленьких компаній, але й для великих.

- **Майданчик для пікових навантажень.** Даний тип хмарного рішення підходить для бізнесу, який має періоди підвищеного навантаження, які можуть чергуватись, або ж це є сезонний бізнес з підвищеним навантаженням. У таких випадках існує можливість винесення у хмару саме тих програмних продуктів, які й використовуються у період пікового навантаження. Це дає змогу організувати гібридну хмару для організації, а інструменти які представлені на ринку для локальних та хмарних інтеграцій, зроблять роботу побудованої інфраструктури ефективнішою.

- **Середовище розгортання для затребуваних проєктів.** Такий варіант використання хмари є досить зручним у випадках, коли при розробці якогось проєкту було упущено деталі чи якісь моменти, або ж не враховано можливі потреби й відповідно на етапі вже розробки проєкту виникає необхідність в

додаткових локальних ресурсах, яких не вистачає. Саме в такий момент на допомогу приходить хмара. Також це чудовий варіант у випадку реалізації проєкту, на який потрібні ресурси, які не є раціональним придбанням для компанії, тоді також можна використати хмару з її представленими ресурсам, що дозволить виконати проєкт та не витрачати лишні кошти.

- **Міграція у хмару всієї інфраструктури**. У випадку, коли компанія обирає мігрувати у хмару повністю, вона може відкрити для себе максимально усі переваги хмарних технологій**.** Звичайно процес міграції не є легким, швидким та дешевим, але воно того варте. У такому випадку, як правило процес міграції на себе бере сам постачальник хмарних послуг, але звичайно це залежить від компанії та потреб. Однією з переваг переходу у хмару, є мінімізація впливу саме на бізнес – процеси, що дає змогу не зупиняти бізнес та втарачти великі кошти, та звичайно оптимізація роботи вже кінцевої інфрастуктури у хмарі. [13]

Існують і інші варіанти міграції, але представдені сценарії є найвживанішими. Хоча і більшість підприємців асоціюють хмару лише з резервним копіюванням даних та це не є всім функціоналом хмарних сервісів і звичайно, що з розвитком нових технологій варіантів використання хмари у бізнесі буде ставати тільки ширшим.

2. Використання хмарних технологій на маркетингових платформах.

З початком використання хмарних технологій, маркетологи, аналітики та інші, значно полегшили свою роботу, оптимізували та звичайно зекономили час, який можуть з користю використати на інших процесах.

Хмарні технології пропонують безліч інструментів для аналітики даних, які дають ефективні результати для роботи маркетолога. Дані інструменти дають можливість швидко розробити та головне оптимізувати маркетингову стратегію. Відповідно робота на маркетингових платформах полегшується. Адже раніше потрібно було спочатку команді зібрати різні маркетингові дані окремо. Тільки після цього процесу у роботу вступила маркетолог та аналітик,

які опрацьовували дані, аналізували й вже далі створювали якусь загальну картину, яка б використовувалась надалі у різних етапах бізнесу.

Хмарні платформи допомагають економити час та кошти компанії й за допомогою інших функцій. Через те, що організації наразі використовують багатоканальні напрямки інформування, зокрема: email-розсилки, соціальні мережі, чат-боти, мобільний зв'язок, месенджери та багато іншого. Саме за допомогою хмарних технологій можливо спростити впровадження та управління процесів інформування клієнтів і не тільки, що спрощує роботу маркетологам.

Варто звернути увагу, що цифровий маркетинг на основі технології SMAC (соціальні мережі, мобільний зв'язок, аналітика та хмарні технології) використовують як сучасну архітектуру великих даних, яка поєднує в собі хмарні, аналітичні, соціальні та мобільні маркетингові впливи, за допомогою яких і підвищують продуктивність бізнесу. Саме ця технологія яка поєднує у собі використання хмарних технологій, є однією з елементів цифрової модернізації маркетингу, який відбувається вже зараз. [15]

Це ще один приклад використання хмарних технологій у сфері маркетингових майданчиків і в загальному в цій сфері. Незважаючи навіть на те, що сфера маркетингу не є представником високотехнологічного напрямку, але спеціалісти з даної сфери побачили всі переваги використання хмарних технологій та віднайшли для себе саме, ті інструменти які допомагають оптимізувати робочі процеси й не тільки. Вже на сьогодні є результати перенесення всього маркетингового відділу у хмару, або ж компанії. Звичайно, що динаміка в майбутньому буде тільки зростати.

3. Сфера освіти, навчальних процесів та науки .

Досить значна частка освітніх навчальних закладів різних рівнів, по всьому світові, вже використовує хмарні технології у різних формах. Звичайно, що Україна не стала винятком, особливо з початком пандемії та надалі повномасштабної війни. Навіть сьогодні, коли навчальні заклади намагаються адаптуватись під умови війни, та переходять на змішаний

навчальний процес, все одно залишається велика частка як школярів, так і студентів, які вимушені навчатись у дистанційній формі.

Саме тому актуальність використання хмарних технологій в освіті залишається не тільки популярною, але й необхідною. Це стосується не тільки навчальних закладів, але й в цілому сфери освіти. Різноманітні курси, навчальні програми, позашкільні процеси тощо, потребують хмарних технологій.

Використання хмарних технологій відіграє значну роль у модернізації педагогічних систем та методів сучасної вищої освіти, що дозволяє формувати та розвивати освітньо-наукове середовище ЗВО. Зокрема використання хмарних обчислень у сфері освіти, дає змогу використовувати більш гнучкі, зрозумілі та головне масштабовані під потреби системи організації доступу до електронної інформації, ресурсів та сервісів. Для усіх учасників освітнього процесу є можливість працювати з програмними продуктами, незважаючи на місцезнаходження, часові обмеження та низку різних чинників.[16]

Усі перераховані можливості є актуальним на сьогодні, так як значна частина як викладачів, так і студентів, а особливо учнів знаходиться за межами України та відповідно деякі мають різницю у часі. Тому хмарні технології допомагають продовжувати навчальний процес та підлаштовуватись під нього.

Відповідно хмарні технології вже зарекомендували себе на всіх навчальних рівнях освіти. Хмарні обчислення використовуються як у школах на різних предметах, так і у фахових навчальних закладах та ЗВО.

4. Охорона здоров’я.

Найбільш активний період переходу в хмару різних сфер охорони здоров’я України відбувся саме з початком всесвітньої пандемії. Зі швидкістю розповсюдження вірусу і відбувався перехід у хмару. Зокрема у проєкті Кабінету міністрів України «Коронавірус в Україні», брала участь українська компанія GigaCloud з постачання хмарних послуг. У рамках проєкту дана

компанія надала хмарний сервіс для розміщення веб-сайту, який став головним інформативним джерелом даних стану пандемії в Україні.

Аналіз даних у сфері охорони здоров’я один із головних аспектів. Саме тому на даній хмарній платформі (https://covid19.gov.ua/) компанія GigaCloud розмістила аналітичний модуль, який збирає дані, аналізує на глибокому рівні та головне надає результат, який висвітлює максимально точно стан протікання пандемії. [17]

Оскільки медичні корпорації для прийняття рішень збирають та аналізують великий обсяг даних, то одним з головних допоміжних засобів виступають саме хмарні технології. Адже за допомогою хмари можна зберегти великий обсяг даних, обмінюватись цими даними з іншими організаціями чи медичними установами та приходити до висновку. Хмарні технології пришвидшують роботу, що є одним з головних аспектів роботи сфери охорони здоров’я, адже від правильного та швидкого розв'язання питання залежать людські життя.

Одним з напрямів використання хмари є впровадження інновацій та цифровізація сфери охорони здоров’я. Досить вагома частка медичних установ як державного, так і комерційного характеру вже впровадили електронні кабінети як лікарів, так і пацієнтів за допомогою хмарних технологій, і не в залежності від місця перебування існує можливість перегляду інформації та історії здоров’я.

Вже сьогодні є результати використання хмарних рішень у медичних закладах для оптимізації робочих процесів. Медичні установи розробляють нові сервіси для роботи у різних напрямках, яка водночас є більш захищеною від витоку інформації, ніж локальні ЦОД, тому це не тільки робота з великим обсягом даних.

Використання хмарних технологій дає можливості обробляти дані як маленьким медичним установам, так і великим на перспективу масштабування. Для сфери охорони здоров’я хмарні рішення допомагають впроваджувати онлайн-бронювання відвідування, електронні кабінети

пацієнтів та лікарів з доступом до інформації, різні елементи телемедицини, і це не кінець списку. [18]

5. Стрімінгові розважальні платформи.

Стрімінгові розважальні платформи вже давно актуальні не тільки у різних країнах світу, але й в Україні. З популяризацією різних технологій та диджиталізацією, зростає і попит на різні стрімінгові платформи, які пропонують різний спектр розважального контенту за підписку.

Саме з використанням хмарних технологій стрімінговими платформами, є можливість слухати музику де завгодно й у будь-який час, з мінімальними умовами для цього. У великої кількості сучасних українців як правило є хоча б одна підписка на стрімінгові платформи, а в деяких навіть і більше.

Завдяки хмарним рішенням, стрімінгові платформи розвивались та розвиваються все більше. Про це свідчать нові можливості та варіанти використання, які пропонують дані сервіси. Ще на початку століття для перегляду фільму чи мультфільму потрібно було додаткове обладнання для того, аби зберегти десь контент для подальшого перегляду. З використанням хмарних технологій на стрімінгових платформах, ця потреба зникла. Адже в хмарі зберігаються тисячі різного контенту, який не потрібно завантажувати.

На сьогодні отримати доступ до серіалів, фільмів або ж телепередач, будь-якого музичного контенту, можна не виходячи з дому, або ж перебуваючи в іншому місті чи країні. Всі матеріали не залежні від часу і головне не потребують різних накопичувачів, все що потрібно це лише пристрій та доступ до мережі.

Це стосується й ігрових стрімінгових платформ, які пропонують підписки на різні ігри у реальному часі, з використанням хмари. Принцип такий самий як на інших стрімінгових платформах, тільки інший напрямок. Після придбання підписки, отримується доступ до бібліотеки у хмарі з іграми. В такому випадку вже не потрібно купувати нові ігри, кожну окремо, а потім їх десь зберігати, тому це зручно та економічно.

Гарним прикладом використання хмари стрімінговою платформою є Netflix. Хмара відкриває не тільки можливості для клієнтів, але й для співробітників. Саме з використанням хмарних потужностей та сервісів, є можливість знімати серіали та кіно з різними спецефектами, які було набагато важче та дорожче реалізувати без хмари. І це тільки одна з можливостей хмари, а їх безліч.

Головною перевагою стрімінгових платформ, все ж є масштабованість, тому що у будь-який момент можна збільшити або ж зменшити ресурси якими ти користуєшся, при цьому заощадити кошти. Через те, що велика кількість стрімінгових платформ використовують хмари, вся інформація зберігається, навіть при умові якщо в якийсь період часу підписка не використовується. [12]

1.6 Переваги та недоліки

Незважаючи на розвиток та популярність, будь-яка технологія включає в себе як плюси, так і мінуси, які визначаються протягом тривалого часу, методами досліджень, застосувань на практиці, аналізу і т.д. Звичайно хмарні технології не стають винятком, тому вони мають вже визначені переваги та недоліки.

З огляду на різні аспекти, плюси та мінуси визначатимуться індивідуально, на це можуть впливати різні фактори, або ж сфера застосування хмарних технологій. Відповідно у сфері освіти та бізнесу, або ж сфері медицини та телекомунікацій переваги та недоліки застосування хмарних технологій будуть відрізнятися, але звичайно, що у будь-якій із цих сфер застосування все ж таки деякі плюси та мінуси будуть збігатися. Саме такі переваги та недоліки будуть найбільш близькі до істини та вимальовувати головні аспекти на які потрібно звертати увагу при виборі.

1.6.1 Переваги

Виділяють ряд переваг, який вже сформувався на протязі значного часу використання хмарних технологій як в іншиг країнах світу, так і в Україні.

Навіть не зважаючи на те, що дана технологія набрала популярність в Україні за останні роки, а не як в інших країних, вже ряд компаній та установ різного характеру, помітили переваги використання.

Найголовнішими перевагами використання хмарних технологій, для різних сфер застування, є:

1. Доступність – користувач підключений до мережі, не в залежності від типу хмари чи моделі сервісу, отримує доступ до хмари та інформації цілодобова. Відповідно відсутні будь які обмеження у часі та місцезнаходжені, що дозволяє оперативно вирішувати питані, що є вагомою перевагою для різних сфер застосування.

2. Економічність – зменшення витрат на різні послуги, такі як утримання додаткового персоналу, закупівлю додаткових програмних продуктів, економія на ресурсах, які вже не використовуються, обладнані різного характеру, як від комп'ютерів та до серверів тощо. Перелік факторів заощадження може продовжувтись, а найголовніше витрати на хмарну інфраструктуру, в квартальному звіті вже покажуть результати економії бюджету в відсотковому співвдношені.

3. Масштабованість – це надання ресурсів за необхідності, з оплатою тільки того, що використовується. Можливість нетільки збільшувати ресурси, але й зменшити у потрібний час. Відбувається без необхідності придбання нової техніки та реалізації приміщення для неї. Завдяки можливості масштабування, можна в будь який момент додати додатковий об'єм оперативної пам'яті, або ж збільшити саме сховище даних.

4. Мобільність – дозволяє співробітникам будь-якої сфери, або ж їх клієнтам отримувати всю інформацію, або ж проводити спілкування з різних питань у режимі онлайн. Це дозволяє пришвидшувати низку процесів, навіть якщо хтось знаходиться у відряджені, або ж де інде. Особлива перевага для дистанційної форми роботи.

5. Гнучкість – одна з найголовніших переваг хмари, тому, що ресурси можна збільшити та зменшити набагато швидше та економічніше, ніж

наприклад, локальні ЦОД. В такому випадку клієнт не тільки заощадить кошти, а й не буде витрачати лишні, за ті потужності, які йому не потрібні.

6. Надійність – у випадку втрати даних з одного серверу, існує можливість отримання доступу до них з іншого. Адже провайдери, які надають хмарні послуги, налаштовують всю свою інфраструктуру з урахуванням забезпечення відмовостійкості на різні випадки, будь то перебої роботи серверів чи збій у резервному копіюванні даних.

7. Безпека – є одним зі спірних плюсів, адже це є вагомою перевагою, якщо вірно налаштувати хмарну інфраструктуру та використати засоби безпеки. У разі помилки це стане фатальним недоліком. Але все ж безпека, незважаючи на все, є одним з найголовніших плюсів хмари. Хмарні провайдери, у свою чергу, пропонують широкий спектр функцій для забезпечення безпеки даних, їх зберігання та обробки.

8. Професійне обладнання – при використанні хмарних технологій, надається можливість користуванням вартісного та потужного обладнання, не купуючи таке професійне обладнання для власної інфраструктури. Що зумовлює збільшення можливостей компанії чи установ, які використовують потужності, для прикладу, при обробці даних, або ж створені якогось програмного продукту тощо.

9. Наскрізний контроль – провайдери весь час шукають недоліки та вдосконалюють надані сервери та послуги. Відповідно у випадку знаходження недоліку відбувається абгрейд продукту та надалі швидке оновлення на стороні клієнта для вирішення неполадок.

Звичайно це не весь список переваг використання хмари, але представлені плюси є найбільш вагомими. Кожен знаходить свої переваги у використанні технологій як на початку, так і упродовж всього користування хмарними технологіями.

1.6.2 Недоліки

Ряд недоліків значно менший ніж переваг і це є гарним показником для технології. Саме тому більшість і обирає використовувати хмарні технології, або ж взагалі переходить у хмару. Кількість недоліків збільшилась у період активного переходу та використання хмари під час всесвітньої пандемії, коли була відсутня можливість працювати в офісі. Чудовим атрибутом є те, що при знаходженні недоліків, постачальники хмарних технологій намагаються якнайшвидше знайти рішення та усунути їх.

До недоліків, які найчастіше зустрічаються та все ще присутні, відносять:

1. Наявність мережевого з'єднання – це є однією з головних проблем, адже без отримання доступу до мережі Інтернет, відсутня можливість користуванням хмарою. Аналогічно й з поганим з'єднанням у мережі виникає проблема у доступі до даних, які зберігаються у хмарі. Так як доступ можна отримати тільки через мережу, відповідно дану проблему вирішити неможливо на даний час.

1. Конфіденційність даних – незважаючи на усі переваги, неможливо бути впевненим на 100%, що дані які передаються між хмарами, або з якими працюють, не будуть розголошені чи переглянуті самим постачальником хмарних послуг. Відповідно, це проблема особливо для документів з грифом секретності, для прикладу. Рішенням проблеми є залучення третьої сторони, але і це не забезпечить повного вирішення.

2. Залежність від постачальника – це є одним з найбільших недоліків, який показує себе, якщо передавати послуги між хмарами різних провайдерів, що може бути навіть не можливим у деяких випадках. Це спричиняє трудності та затримки у роботі. На це впливають різні політики безпеки, або ж різні налаштування платформ та самої хмари у постачальників, що зумовлює просто не сумісництво роботи та унеможливлює роботу у хмарі з різними постачальниками хмарних послуг одночасно.

3. Не повний контроль – так як у більшості випадків контроль над усією хмарною інфраструктурою лежить на постачальникові хмарних послуг

і у випадку проблеми контролю чи керування, користувач не може нічого вдіяти. Відповідно вся відповідальність припадає на третю сторону, що у деяких випадках стає проблемою для компанії чи установи. Тому, що користувачі не мають повного контролю над їх інфраструктурою та у випадках ризику повинні покладатись лише на компетентність та професіоналізм хмарного провайдера.

4. Безпека – незважаючи, що це є і перевагою, це також виступає і недоліком. Головною проблемою є елементарна втрата конфіденційної інформації у процесі передачі їх у саму хмару через третю сторону, тобто самого постачальника хмарних послуг. Звичайно, що провайдери використовують та впроваджують найкращі стандарти безпеки, але й розвиток у сфері хакерства також не стоїть на місці. Тому звичайно ризик втрати даних чи контролю навіть над хмарою не зникає.

Висновки до розділу 1

В першому розділі було проведено аналіз існуючих понять «хмарні технології» та визначено найоптимальніший варіант, що в подальшому дало змогу обґрунтувати актуальність використання саме хмарних технологій у різних сферах життя.

Перший розділ вмістив у себе огляд сучасних технологій хмарних обчислень з описом моделей та типів хмарних обчислень. Було ретельно розглянуто сфери застосування хмарних обчислень у різних сферах життя на сьогоднішній день, з прикладами та принципами застосування та перспективою на майбутнє. Проведено аналіз плюсів та мінусів хмарної інфраструктури у різних сферах використання та визначено найбільш схожі для всіх сфер, з уточненнями чи можливо уникнути недоліків у майбутньому.

РОЗДІЛ 2. Проєктування хмарної інфраструктури для інтернет магазину на базі AWS

2.1 Створення та налаштування акаунту в системі AWS

Для подальшої взаємодії із системою AWS необхідно створити акаунту у даній системі. Використання акаунту надасть можливість більш детально проаналізувати існуючі сервіси AWS та розділити їх на основні підкатегорії, які будуть розглядатись надалі. Звичайно найголовніша функція акаунту AWS полягає у надані необхідних послуг та сервісів у користування. Використовуючи акаунт, буде підібрано низку сервісів, які будуть закривати потреби проєкту та на основі яких буде побудована архітектура хмарної інфраструктури та в подальшому реалізується.

Створення акаунту відбувається у декілька кроків, для початку необхідно натиснути відповідну кнопку “Create an AWS Account”, як показано на рисунку 2.1.1, та обведено червоним прямокутником.

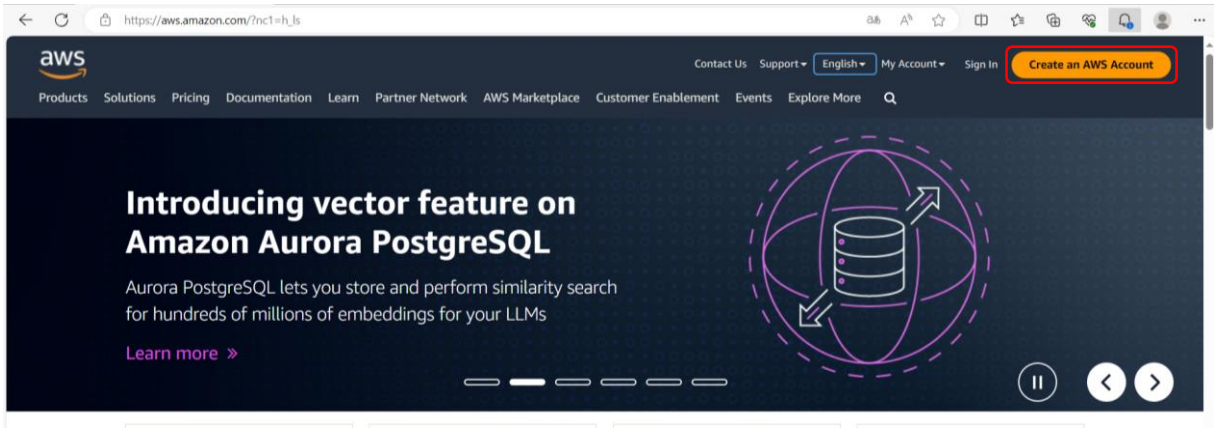

Рисунок 2.1.1 – Створення акаунту в системі AWS

Далі обираємо створення root користувача, тобто головного. Після цього починається етап реєстрації безкоштовного акаунту, який складається з 5 кроків. На першому кроці необхідно вести електронну адресу як на рисунку 2.1.2, за допомогою якої буде відбуватись вхід в акаунт в подальшому. Після того як обрано електронну адресу, необхідно перевірити чи вона справжня, натиснувши відповідну кнопку “Verify email address”.

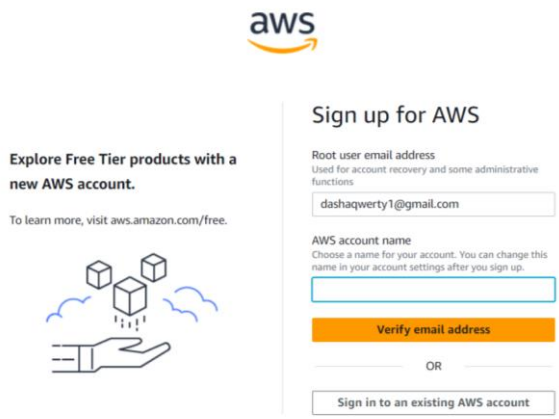

Рисунок 2.1.2 – Обрання електронної адреси для подальшої роботи з AWS

Якщо з електронною адресою немає жодних проблем, на неї прийде лист, як на рисунку 2.1.3, з кодом для підтвердження, що саме дана електронна адреса буде використовуватись створеним акаунтом.

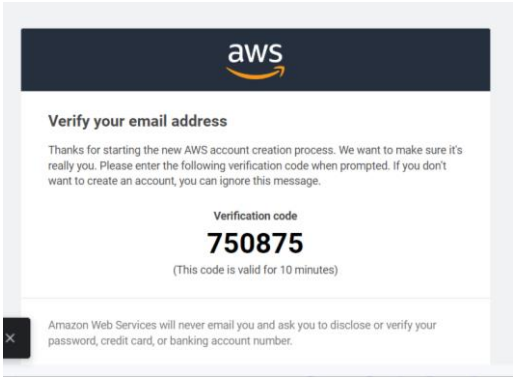

Рисунок 2.1.3 – Лист з кодом підтвердження електронної адреси

Після отримання коду для підтвердження, необхідно повернутись до процесу реєстрації акаунту та вести його у відповідне поле для перевірки, як на рисунку 2.1.4.

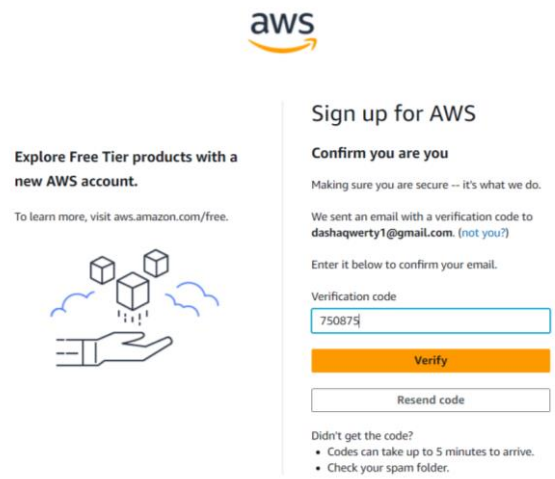

Рисунок 2.1.4 – Перевірка вказаної електронної адреси

Далі відбувається перевірка і якщо код проходить верифікацію, то процес реєстрації переходить на наступний крок, як на рисунку 2.1.5. Також висвічується повідомлення, що це насправді Ви та Ваша електронна адреса пройшла процес перевірки.

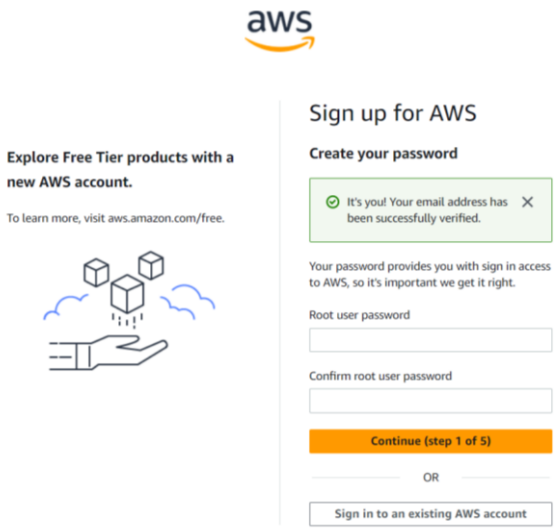

Рисунок 2.1.5 – Перехід на наступний крок реєстрації

На другому кроці необхідно придумати надійний та комплексний пароль, який буде відповідати усім правилам сильного паролю, що забезпечить безпеку від несанкціонованого доступу до акаунту, як показано на рисунку 2.1.6.

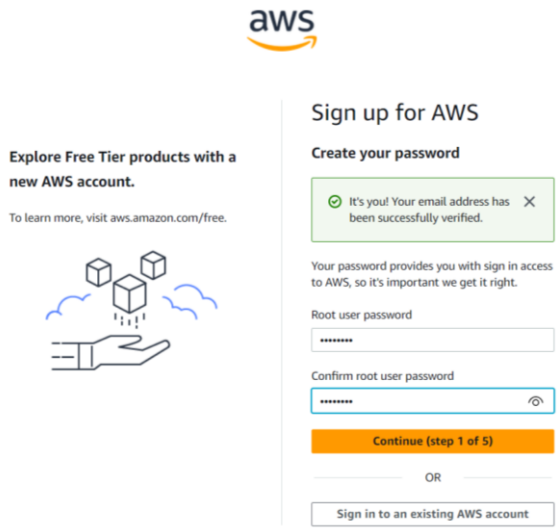

Рисунок 2.1.6 – Другий крок реєстрації, вибір паролю

Після того, як пароль обрано відбувається перехід на наступний крок, тобто третій, на якому необхідно заповнити конфіденційну інформацію, як на рисунку 2.1.7 та рисунку 2.1.8. На даному етапі заповнюється наступна інформація: обрання виду акаунту(в нашому випадку персональний, для особистого проєкту), ім’я та прізвище, номер телефону(для безпеки замальований), адреса проживання яка прив’язана до кредитної карти та дані карти для реєстрації акаунту для оплати подальших послуг(не показано, у цілях особистої безпеки).

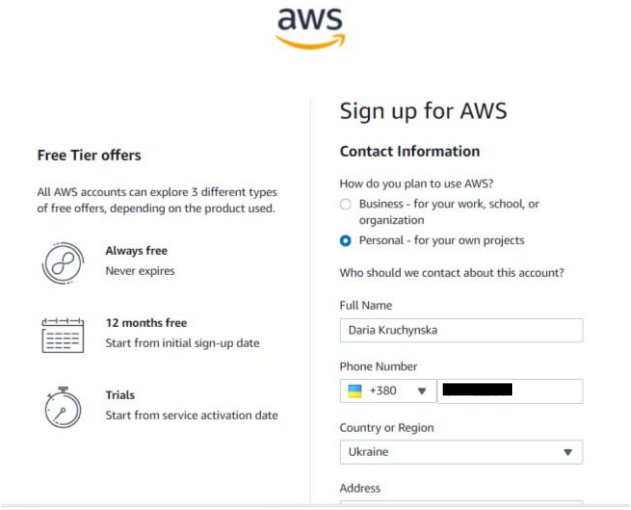

Рисунок 2.1.7 – Третій крок реєстрації, заповнення конфіденційної інформації

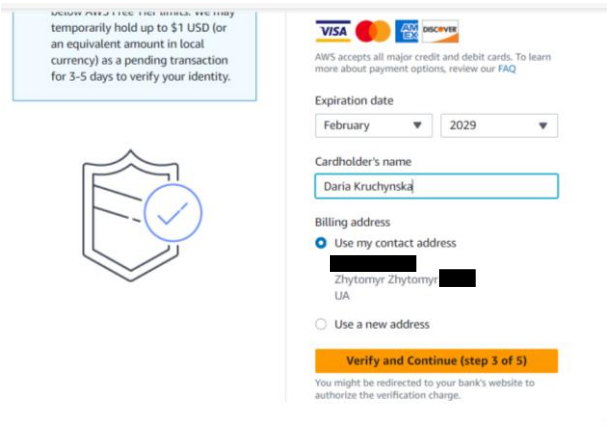

Рисунок 2.1.8 – Продовження заповнення конфіденційної інформації

На четвертому етапі реєстрації відбувається підтвердження особистого номеру телефону, як на рисунку 2.1.9, в цілях безпеки він замальований. Перевірка відбувається шляхом відправлення коду на вказаний номер телефону, але перед цим необхідно для додаткових цілей безпеки ввести капчу. Після того, як всі поля заповнені, натискається відповідна кнопка для відправки смс повідомлення.

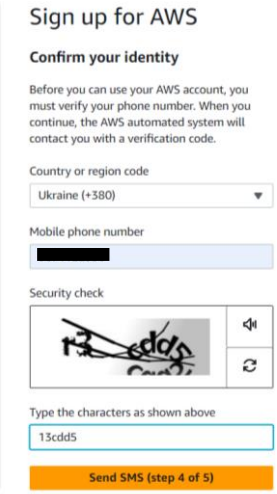

Рисунок 2.1.9 – Четвертий крок реєстрації, введення інформації для перевірки мобільного телефону

Після отримання повідомлення продовжується все ще четвертий крок реєстрації акаунту на якому необхідно ввести отриманий код у відповідне поле для подальшої перевірки, як на рисунку 2.1.10, та натиснути відповідну кнопку.

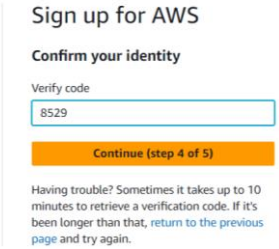

Рисунок 2.1.10 – Четвертий крок реєстрації, введення коду для перевірки

Якщо всі кроки були вірно заповнені та успішно проведені всі верифікації електронної адреси та мобільного телефону, відбувається перехід на останній п’ятий крок реєстрації акаунту, як на рисунку 2.1.11, висвічується повідомлення про успішно зареєстрований акаунт та пропонується перейти на панель керування.

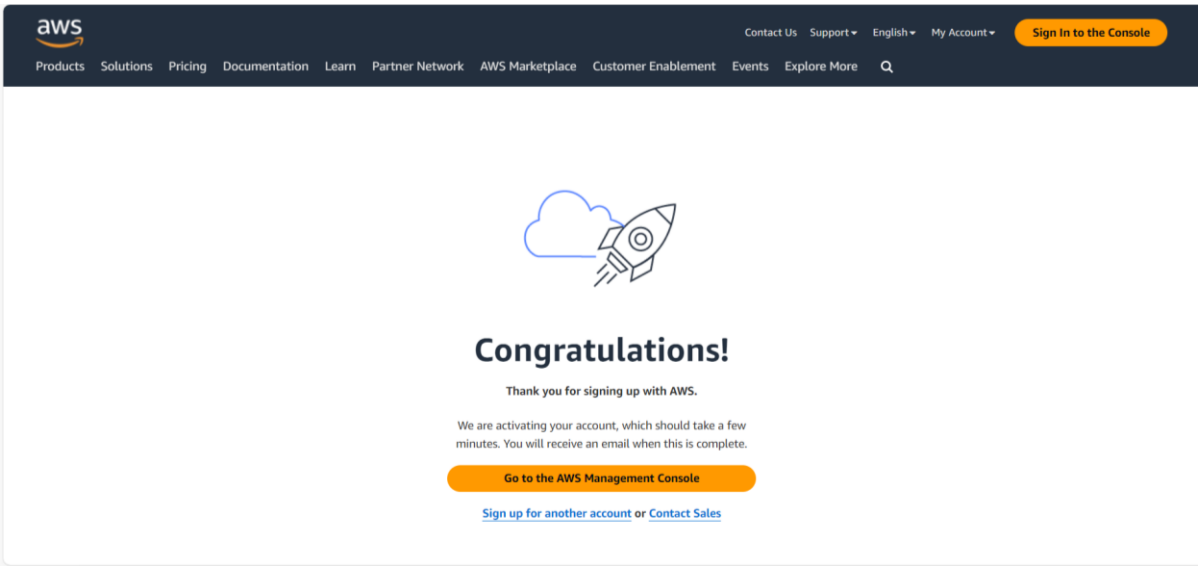

Рисунок 2.1.11 – Успішно зареєстрований акаунт в системі AWS

Далі можна перейти на панель управління для перевірки чи реєстрація відбулась, як на рисунку 2.1.12. На разі вона пуста, але в подальшому тут буде реалізовуватись архітектура хмарної інфраструктури.

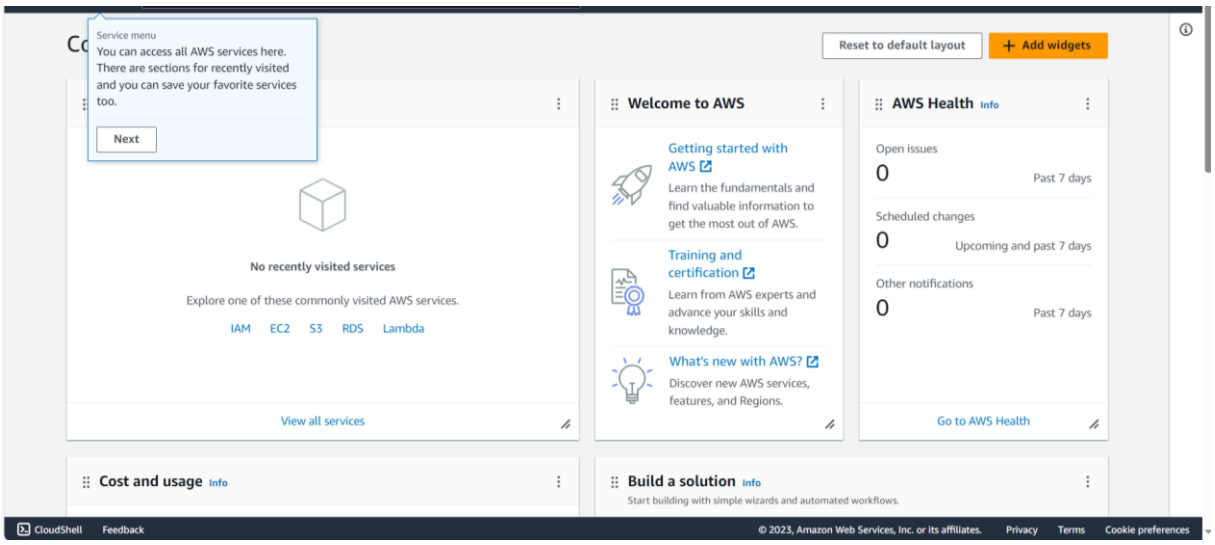

Рисунок 2.1.11 – Панель керування

2.2 Класифікація та аналіз принципів функціонування базових веб-сервісів в системі AWS

З аналізу різних статей та досліджень, як вітчизняних, так і зарубіжних, та роблячи висновок, Amazon Web Services (AWS) все ще залишається лідером серед інших. З різних статистик за минулі роки AWS охоплює понад 30 відсотків світового ринку та є номером один серед конкурентів. Саме тому в першу чергу увагу звертають на AWS.

Для початку, AWS – постачальник хмарних послуг, який являє собою онлайн – платформу, для надання користувачам готового функціоналу для використання у своїх цілях. Під функціоналом може бути як сховище, так і обчислювальні ресурси які необхідні для роботи, або ж ціла інфраструктура та сервіси.

Тобто даний функціонал надає можливість орендувати саме ті віртуальні онлайн ресурси, які потрібні зараз, що дає в свою чергу варіант заощадження коштів, через те, що відкидається потреба у придбані фізичних ресурсів чи обладнання.

Веб-сервіси Amazon(AWS) – це повний комплект віддаленого обчислювального обслуговування, що забезпечує хмарну інфраструктуру

через мережу зі збереженням, спеціалізованою підтримкою інтерфейсів програмування прикладних програм (API) та пропускною здатністю.

На сьогодні нараховується вже понад 200 різноманітних веб-сервісів Amazon, для різних сфер, які відрізняються за призначенням та різними характеристиками. Всі сервіси можна умовно класифікувати під різні розділи.

Класифікація видів сервісів AWS:

- сервіси для виконання обчислень та безсервісні обчислення;
- сховища даних;
- хмарні БД з можливостями СУБД;
- віртуальні мережі та доправлення контенту;
- аналітичні сервіси;
- адміністрування та управління хмарою;
- машинне навчання;
- та інші.

Сервіси для виконання обчислень та безсервісні обчислення

Значна частина користувачів, коли мова заходить про хмару, одразу згадують про платформу, як різноманітні області обчислень для різного роду навантажень. Звичайно, що сервіси обчислень займають не останнє місце у різноманітності сервісів. Велика кількість компаній із року в рік запускають різноманітні робочі навантаження на обчислювальних платформах, які надає AWS.

Однією із найголовніших переваг сервісів обчислення AWS, перед іншими хмарними провайдерами, є те, що даний провайдер надає стабільний набір послуг із хмари до потрібного центру обробки даних і звичайно на периферійні пристрої. Найголовніше, що все це клієнт отримує тоді, коли це необхідно і саме в тому місці, що звичайно пришвидшує обробку, роботу даних і т.д. для будь-якої сфери.

Взагалі обчислювальні сервіси розділяють умовно на підкатегорії:

- Віртуальні машини (Amazon EC2, AWS Batch та ін.). Використовуючи сервіси обчислень з даної підкатегорії, користувач може не тільки розміщувати дані, розробляти додатки, або ж розгортати їх, а й тестувати те що потрібно. Однією з переваг є використання орендованого обладнання при необхідності;
- Безсервісні обчислення (AWS Lambda). В основі даних обчислень є запуск додатків, або ж коду і т.д. без керування сервісами, при тому, що кошти знімаються по мірі використання, що оптимізує бюджет та додає гнучкості;
- Контейнери (AWS App Runner, Amazon Elastic Conteiner Service та ін.). Дані сервіси спрощують запуск контейнерів та додатків на основі контейнерів. Різноманітність сервісів пропонує запуск контейнерів як з керуванням сервісу, так і без, та різноманітні сервіси для оркестрації;
- Управління витратами та ресурсами (AWS Compute Optimizer, Elastic Load Balancing (ELB) та ін.). Саме сервіси з даної категорії, за рахунок гнучкої моделі ціноутворення, підбору оптимальних ресурсів, автоматизації процесів тощо, допомагають не тільки зменшити витрати при використанні обчислювальних ресурсів, а й збільшити продуктивність робочих навантажень;
- Гібридна та периферійна архітектура (AWS Local Zones, AWS Outposts та ін.). Використовуючи обчислювальні сервіси з даної підкатегорії, користувач має можливість запускати такі додатки, які є чутливими до затримок та мають різний ступінь робочих навантажень, що є актуальним на сьогодні.

Сховища даних використовуються вже не один рік безліччю клієнтами, більшість із них навіть й асоціюють хмарну інфраструктуру тільки із хмарними сховищами, але звичайно це не тільки вони. Використовуючи сервіси сховищ даних, відповідно до тих потреб, які висуваються клієнтом, отримується функціонал сховищ даних, захист та аналіз інформації, яка безпосередньо буде переміщена у хмарне сховище і звичайно доступ до цих даних.

Сервіси які представляють собою сховища даних, налічуються більш як 10 і кожен з них має свої можливості, тому їх можна розділити на підрозділи:

- об’єктні, файлові та блокові сховища (Amazon Simple Storage Service(Amazon S3) та ін.);
- гібридне хмарне збереження та обчислення на периферійних пристроях(AWS Storage Gateway та ін.);
- резервне копіювання та аварійне відновлення(AWS Backup та ін.);
- кероване передавання даних(група сервісів AWS Transfer);
- міграція даних(AWS DataSyns та ін.).

Різноманіття сервісів пов'язаних, сховищами даних, надають можливості закривати досить різні потреби для будь-якої сфери. Існує достатня кількість варіантів застосування сервісів хмарних сховищ, найпоширенішими є:

1. *Резервне копіювання в сховище AWS.* Саме за допомогою сервісів та додаткових партнерів AWS є можливість не тільки перенести копії локальної інформації, а й захистити додатки які вже перебувають у хмарі. Дані можливості дозволяють збільшити цільові вторинні сховища у хмарі, що в свою чергу вирішує проблему швидкого та нестримного зростання обсягу інформації, що є важливим для специфічних сфер застосування і не тільки.
2. *Міграція додатків у сховище.* За допомогою сервісів AWS можна перемістити у вихідному вигляді різноманітні додатки, наприклад, мережі зберігання даних (SAN), мережеві сховища (NAS) тощо, та продовжувати працювати з ними у власному ритмі. Міграцію можна виконувати швидко, повторно розміщуючи вже існуючі робочі навантаження та використовуючи подібне сховище для міграції у саму хмару.
3. *Архівування у сховищі даних.* Сервіси AWS з категорії сховищ даних, забезпечують довгострокове зберігання даних, яке необхідно будь-де. В архівуванні даних у сховищі є перевага перед локальними сховищами, у швидшому доступі до даних і не в залежності від місця перебування. З використанням даних сервісів, можна контролювати збереження цифрової

інформації та контролювати вимоги до даного процесу, що забезпечує надійність, безпеку та найголовніше масштабованість.

4. *Створення озер даних.* Використовуючи відповідні сервіси створюються озера даних, які є безпечними, масштабованими та надійними. Саме дана можливість допомагає об’єднати інформацію так, як цього потребує саме клієнт та надалі, наприклад, аналізувати чи моделювати дані які вже є в озерах, а оскільки вони вже розподілені, то це стає набагато простіше та швидше. Додатково створені озера даних досить легко інтегруються із різноманітними сервісами, такими як, наприклад, машинного навчання тощо.

5. *Обробка даних у місцях без можливості живлення.* У відключених від постачання живлення, або ж специфічно захищених місцях, саме за допомогою фізичних пристроїв AWS існує можливість запуску необхідного додатку. Тому дані можна не тільки зібрати та обробити, а й мігрувати у хмару, використовуючи відповідні сервіси, які продовжують працювати не зважаючи на важкі та навіть не передбачувані умови, що дозволяє бути мобільним і не тільки.

Саме використання сховищ даних, може допомогти бізнесу чи сфері діяльності перейти на новий рівень, більш інноваційний та зручний, що в подальшому дає змогу зменшити витрати, збільшити гнучкість даного бізнесу та пришвидшити впровадження інших інновацій. Всі ці аспекти допомагають бізнесу залишатись конкурентоспроможним на ринку.

Хмарні БД з можливостями СУБД

Бази даних є невід’ємною частиною будь-якого підприємства, організації, програмного продукту тощо. Інформації з кожним днем стає все більше і більше, тому використання хмарних БД є вирішенням великої низки проблем, з якими стикаються при організації роботи. Хмарні БД приходять на допомогу при модернізації інфраструктури вже існуючої інформації та з перспективою на майбутнє, адже мають функціонал для управління спеціалізованих БД.

Зважаючи на те, що більшість технологій для компаній це додаткові витрати, які не завжди є раціональними, або ж вимагають більше витрат, тому

деякі компанії мають сумніви чи готові вони до впровадження нових інновацій. Що стосуються хмарних БД, то в цьому випадку компанія отримує не тільки нові інноваційні можливості, а й зменшує свої витрати, в залежності від реалізації інновацій чи обрання сценарію від старого до нового, можна заощадити від 10% до 90% бюджету.

Існує більше 10 різновидів сервісів хмарних БД, їх умовно розділяють на підкатегорії за типами БД:

- Реляційні БД (Amazon RDS та ін.). Дані БД використовуються в інтернет комерціях, для планування корпоративних ресурсів тощо;
- БД часових рядів (Amazon Timestream). Найчастіше обирають для роботи у DevOps та додатках інтернету речей(IoT), але і це не кінець списку;
- Документові БД (Amazon DocumentDB (підтримують сумісність з MongoDB)). Як правило в них зберігаються профілі користувачів, каталоги й також їх використовують для керування контентом;
- Графові БД (Amazon Neptune). Їх використовують для пошуку шахрайства, також у соціальних мережах і не тільки;
- БД на основі пар “ключ-значення” (Amazon DynamoDB). Найчастіше вибір падає на дану БД для використання в ігрових додатках, або ж Web-додатках які мають високий трафік переміщення даних;
- БД для реєстрів (Amazon Quontum Ledger Database (QLDB)). Будь-яка державна установа має свої реєстри, тому найбільше даний сервіс підходить для цієї сфери. Але також це можуть бути банківські транзакції, будь-які системи запису в різноманітних сферах тощо;
- Колонкові БД (Amazon Keyspaces). Вибір даного сервісу доцільний, наприклад, для масштабованих промислових додатків у технічному обслуговуванні обладнання, але звичайно це не єдиний варіант для даного сервісу;
- БД у пам’яті (Amazon MemoryDB for Redis та ін.). Ідеально підходять для кешування інформації й не тільки, керування сесіями тощо. Актуальне використання у геопросторових додатках.

Обираючи сервіси хмарних БД відповідно до потреб та очікуваних результатів здійскюється перехід до керованих БД, що дозволяє автоматизувати управління та масштабування баз даних. Переходя до нового, нарешті є можливість відмовитись від старого, тому можна відмовитись від використання комерційних БД.

Віртуальні мережі та доправлення контенту включає в себе набір різноманітних сервісів, як для мережевих сервісів, так і для доправлення контенту в різні точки світу. Використання віртуальних мереж дає можливість запустити будь-яке робоче навантаження, а найголовніше, що безпечним шляхом, і завдяки цьому клієнт отримує надійність та високу продуктивність своєї глобальної мережі.

Всі сервіси у даній категорії можна також додатково поділити, умовно на підкатегорії. Дані підкатегорії будуть представлятися як:

- застосування мережевих технологій (Amazon API Gateway та ін.);
- робота в периферійних геопозиціях мережі (Amazon CloudFront та ін.);
- основні положення про мережу (Amazon VPC та ін.);
- гібридні підключення (AWS Site-to-Site VPN та ін.);
- мережева безпека(AWS Firewall Manager та ін.).

Після обрання клієнтом саме тих сервісів із даної категорії, які закривають потреби бізнесу, можна отримати:

1. *Безпеку.* Це стосується як цілісності, так і доступності всіх даних, а найголовніше конфіденційності, що не дасть змоги для реалізації витоку даних. Оскільки AWS використовують та дотримуються найсуворіших правил безпеки у мережевій галузі, як, наприклад цілодобовий моніторинг тощо.

2. *Доступність мережі.* Існує можливість реалізувати найвищий рівень доступності саме для критично важливих елементів бізнесу, які мають високий рівень навантажень, використовуючи, наприклад модель зон доступності.

3. *Широке глобальне покриття.* AWS як постачальник хмарних послуг, має додаткову перевагу перед іншими постачальниками, за рахунок

найбільшої глобальної інфраструктури. Це дає можливість доставити швидко та надійно додатки або ж контент, за допомогою саме спеціалізованої мережі, у будь-яку частину світу.

4. *Висока та стабільна продуктивність.* Використовуючи віртуальні мережі, клієнти мають можливість надавати своїм користувачам швидкі та автоматизовані додатки. Тому користувачі отримують найбільшу пропускну здатність та найменшу затримку, що позитивно впливає на будь-який бізнес.

Аналітичні сервіси мають широкий асортимент, який задовольнить більшість клієнтів, які мають потребу в аналітиці даних. Використовуючи аналітичні сервіси, користувач не тільки в найменший час отримає всі відповіді, які очікує від аналізу всього масиву даних, але й зможе створити бізнес з нуля після отриманих даних, незважаючи будь то маленький чи великий, та сферу реалізації.

Сервіси аналітики класифікують на категорії за областю застосування даних рішень. Виділяють 3 категорії:

1. Розширена аналітика. У даній категорії представлений широкий асортимент сервісів, які налічують більше 10 та є вигідними для компанії, зважаючи на фінансову сторону. За допомогою сервісів можна швидко отримати результати, які цікавлять за даними компанії. Сервіси з розширеної аналітики використовуються різноманітними варіантами:

- в операційній аналітиці(Amazon OpenSearch Service);
- в аналітиці, яка відбувається в режимі реального часу (Amazon Managed Service for Apache Flink);
- для інтерактивної аналітики (Amazon Athena);
- у підготовці візуальної інформації (Amazon Glue DataBrew);
- тощо.

Розширена аналітика поєднує у собі 3 різні аспекти, які є важливими для будь-якої компанії, підприємства, державної установи тощо. Одним із найголовніших все ж є *співвідношення ціни та продуктивності*. Адже вартість

проєкту та очікуванні результати є одними з найголовніших тому, що досить часто проєкт закривається ще не почавшись із-за досить високої вартості.

На другому місці можна виділити *зменшення часу простою та покращення використання доступних потужностей*. Час у будь-який справі є одним з найцінніших ресурсів. При використанні різноманітних функцій, або ж обладнання тощо, виникає потреба максимально зменшити години простою, адже це кошти, ресурсу і т.д. Використовуючи сервіси AWS можна не тільки швидко виявити проблему, але й так же швидко її усунути.

І останнє це *широкий вибір сервісів* для даної категорії. Таке розташування даного аспекту, обґрунтовуються тим, що незважаючи на широкий вибір сервісів, якщо перші два аспекти відсутні, то третій має досить малий вплив на вибір клієнта, на користь хмарного провайдера AWS.

2. Керування даними. В аналітиці будь-якого характеру не обійтись без керування даними. У категорії управління інформацією налічується понад 10 сервісів. Використання сервісів керування даними допомагає не тільки просто переміщувати дані між різними сховищами та озерами даних, а й об’єднувати та виконувати реплікацію даних.

Сервіси управління інформацією застосовуються у багатьох випадках, наприклад:

- в об’єктних сховищах та озерах даних(AWS Lake Formation та ін.);
- для переміщення даних у режимі реального часу (Amazon Kinesis Data Streams та ін.);
- для управління даними (AWS Glue та ін.);
- тощо.

Управління інформацією відіграє важливу роль у багатьох випадках та вирішує низку питань, які постають перед клієнтом. Використовуючи сервіси керування даними, відповідно до потреб компанії в аналітиці, допомагає *більш швидко інтегрувати дані* для подальшої роботи. Дана можливість є вагомою перевагою, особливо у бізнесі, так як багато компаній цінує свій час та своїх співробітників.

Також необхідно зауважити, що дані сервіси вирішують питання *гнучкості та швидкості* отримання даних. У цьому випадку доступні сервіси допомагають зберігати дані, незважаючи на їх формат та об'єм в одному місці, за рахунок чого в подальшому швидко можна витягнути потрібну інформацію.

Систематизація та аналіз різноформатних даних із декількох джерел відбувається легко та швидко, за рахунок *масштабування* даних джерел до потрібного розміру, в залежності від потреб саме на цей час. Це все надалі допомагає автоматизувати потрібні задачі для аналізу та отримання результатів.

3. Прогнозована аналітика та машинне навчання. Саме для прогнозованої аналітики використовується широкий набір сервісів машинного навчання і звичайно інструментів, які працюють з озерами даних. Прогнозована аналітика використовує сервіси платформ (Amazon SageMaker) та фреймворки й інтерфейси (AWS Deep Learning AMIs).

При роботі з даними сервісами клієнт отримує вбудовану *інтеграцію машинного навчання* у своїх аналітичних сеірвісах та відповідно спеціалізованих сховищах даних, що дозволяє створювати, навчати та розвертати моделі, які необхідні для аналітики.

Використовуючи аналітичні сервіси, які в свою чергу користуються перевіреними можливостями машинного навчання, користувачеві в кінцевому результаті, *швидко та більш докладно,* надається уявлення про дані. Ну і звичайно найголовнішою перевагою залишається *співвідношення ціни та ефективної продуктивності* всіх аналітичних сервісів.

Адміністрування та управляння хмарою містить широкий набір сервісів, які допомагають виконувати моніторинг, розподілення, автоматизацію всіх компонентів у хмарі та багато іншого. Використовуючи усі можливості даних сервісів можна організувати кероване управління, що при цьому не буде впливати на час розробки продукту та створювати затримки відповідно. Дану категорію сервісів можна розбити на 4 підкатегорії:

1. *Управління системами.* AWS пропонує сервіси для управління операціями та системами, які дозволяють реалізувати не тільки контроль над ресурсами хмарної інфраструктури, а й керівництво цим процесом, який буде відповідати потребам замовника. Сервіси управління системами пропонують різноманітний функціонал, такий як, реєстрація дій користувачів у системі, автоматизація задач, моніторинг ресурсів, управління хмарними операціями тощо (AWS Systems Manager та ін.).

2. Розподілення ресурсів. Процес розподілення ресурсів є важливим, а виконання його повинно бути логічним, аби не платити лишні кошти й не тільки. Використання сервісів з даної категорії, може автоматизувати процес розподілення всіх ресурсів у хмарній інфраструктурі та навіть створити колекції ресурсів, використання яких дозволено, наприклад у декількох підрозділах компаній, тобто іншими словами це навіть може бути як політика, яка спростить та пришвидшить процес роботи (AWS CloudFormation та ін.).

3. Управління сервісами для керування конфігураціями. Автоматизація будь-якого процесу є невід'ємною частиною для будь-якої хмарної інфраструктури, адже це пришвидшує процес, економить кошти та звільняє від помилок, звичайно не у всіх випадках, але в більшості. Використання сервісів для керування конфігураціями звільняє в першу чергу від користування власними такими системами, звільняє бюджет, та від турбот масштабування пов'язаних інфраструктур (AWS OpsWorks та ін.).

4. Моніторинг та введення журналів. Моніторинг є важливим зважаючи на різні фактори, такі як, безпека, аналіз, оптимізація тощо. Використовуючи сервіси для моніторингу, важливим є те що вони взаємодіють з іншими сервісами, що дозволяє більш точно вести журнали моніторингу та надалі виконувати аналіз тощо (Amazon CloudWatch та ін.).

Важливо, що сервіси цих чотирьох категорій взаємодіють між собою та з іншими сервісами AWS, що дозволяє автоматизувати та зробити хмарну інфраструктуру, ще більш керованою та з більшими можливостями.

Відповідно контролювання всіх сервісів хмарної інфраструктури стає, ще більш легким, що позитивно вплине на будь-яку сферу.

Машинне навчання надає можливість швидко застосовувати інновації у своєму бізнесі використовуючи набори сервісів як машинного навчання, так і штучного інтелекту (AI). З використанням у бізнесі машинного навчання отримується більш глибоке уявлення про дані які використовуються, при цьому зменшуються витрати, що є гарним показником для будь-якого бізнесу чи сфери діяльності.

На сьогодні існує більш як 30 різноманітних сервісів, які базуються на машинному навчанні, наприклад Amazon Monitron, Amazon DevOps Guru, Amazon Personalize тощо. І головне, що розробка сервісів які базуються чи працюють з машинним навчанням, продовжується і сьогодні, і тільки набирає все більше популярності.

Сервіси машинного навчання вирішують низку потреб, проблем чи питань та можуть бути задіяні у найрізноманітніших сферах, або ж реалізовуватись у різних інтерпретаціях, зокрема:

- розширювати можливості для різносторонніх додатків;
- розв'язання різносторонніх задач у будь-якій сфері;
- прогнозування без написання коду;
- створення, розгортання та навчання моделей для різноманітного використання;
- програмування застосунків із генеруючим штучним інтелектом;
- тощо.

Сервіси які працюють з машинним навчанням можна розділити на підкатегорії, як і більшість інших, адже їх кількість вражає, та кількість питань які вони вирішують різняться, тому сервіси машинного навчання поділяються на:

- промисловий штучний інтелект (Amazon Monitron та ін.);
- комерційні метрики (Amazon Forecast та ін.);

- аналіз та автоматизоване представлення даних (Amazon Comprehend та ін.);
- машинний зір (Amazon Rekognition та ін.);
- покращення взаємовідносин з клієнтами (Amazon Personalize та ін.);
- програмний код та DevOps (Amazon CodeGuru Reviewer та ін.);
- охорону здоров'я (Amazon Healthlake та ін.)

Відповідно сервіси AWS машинного навчання мають найширший та найглибший набір сервісів, який підходить як розробникам, дослідникам, так й іншим спеціалістам різних галузей. Тобто сервіси штучного інтелекту застосовуються майже усюди, і звичайно що цей напрямок та розробка нових сервісів машинного навчання буде тільки все більше розвиватись, а набір сервісів розширюватись.

2.3 Аналіз елементів захисту інформації в системі AWS

Захист робочих навантажень, додатків та ресурсів розташованих у хмарі є важливим. Тому дана категорія сервісів розглядається більш детально. Оскільки незважаючи на популярність хмар та вже реалізованих проєктів, все ще існують користувачі які не впевнені у безпеці хмари. Навіть зважаючи на той факт, що масштабних проблем безпеки хмари не було на даний час.

Звичайно, що недовіра користувачів є нормальним фактором, адже хакерські атаки, створення нових методів та засобів заволодіння інформацією, зловмисне ПЗ, яке наносить шкоду, це все розвивається кожен день. А вирішення проблем безпеки не зважаючи на свій темп розвитку, все ж таки відстає у деяких моментах.

Усі сервіси, які реалізують безпеку в системі AWS, можна розбити та 5 категорій та розглянути більш детально, адже сервісів для захисту хмарної інфраструктури й не тільки налічується більше 20 і розробка нових не стоїть на місці. При чому вже існуючі сервіси продовжують вдосконалюватись.

1. Виявлення та реагування. Безперервне виявлення загроз для безпеки є важливим елементом, а найголовнішим – реагування на виявлення

інцидентів, для того аби забезпечувати ефективний захист робочих навантажень не зважаючи на масштаб. Сервіси виявлення та реагування AWS, взаємодіють між собою, що дозволяє підвищити рівень захисту та оптимізувати процес організації безпеки у всіх хмарній інфраструктурі й не тільки. Використовуючи дані сервіси, можна реалізувати такі види захисту:

- *Розслідування, швидке реагування на інциденти безпеки та подальший захист.* Вірна розстановка пріоритетності сповіщення, організація сортування та аналіз відсортованих даних, для визначення причин загроз безпеці, всі ці етапи допоможуть організувати захист в першу чергу для критично важливих робочих навантажень у хмарі.

- *Виконання централізованого моніторингу для прискорення виявлення потенційних ризиків.* Використовуючи агрегування даних в інфраструктурі можна підвищити прозорість безпеки, що надалі допоможе автоматизувати дії для забезпечення безпеки та моніторингу стану хмарного захисту.

- *Захист робочих навантажень власної інфраструктури від небезпек.* Невірно налаштовані хмарні ресурси, без урахувань рекомендації із безпеки, є одним із факторів загроз, який необхідно моніторити та перепровіряти й звичайно слідкування за оновленнями, адже кожне ПЗ має моменти з порушеннями безпеки, які при оновленнях виправляються.

- *Використання інноваційних підходів для гібридних середових.* Організувавши об’єднання даних безпеки із хмарних та локальних джерел, можна отримати цілісне уявлення про безпеку гібридної інфраструктури в цілому, що є зручним для подальшого розслідування інцидентів у випадках їх виникнення.

До сервісів першої категорії можна віднести наступні:

- Amazon Inspector – керування вразливостями у великих масштабах, яке відбувається безперервно та автоматизовано.
- Amazon Security Lake – централізована автоматизація даних безпеки.
- AWS Security Hub – автоматизація перевірок системи та отримання результатів, таких як попередження від систем безпеки.

- Amazon GuardDuty – використовуючи логічне виявлення загроз для захисту облікових записів AWS.
- AWS IoT Device Defender – керування безпекою пристроїв IoT.
- AWS Config – аналіз, оцінка та перевірка конфігурації особистих ресурсів AWS.
- AWS CloudTrail – використовується для використання API та відстеження дій користувачів.
- Amazon Detective – застосовується для виявлення потенційних проблем захисту за допомогою аналізу та візуалізації конфіденційної інформації.
- AWS Elastic Disaster Recovery – економічне та масштабоване відновлення додатків в AWS.
- Amazon CloudWatch – реалізовує процес слідкування за станом ресурсів та застосунків в AWS, як в локальній частині, так і в хмарній для подальшого аналізу.

2. Захист даних. Конфіденційність та захист даних є чи не однією з головних проблем будь-якої системи. Набір сервісів від AWS який використовується для захисту особистих даних, реалізовує паралельно захист облікових засобів та робочих навантажень від несанкціонованого доступу, оскільки всі ці процеси є взаємопов'язаними. Використовуючи даний набір сервісів, в залежності від потреб, користувач може реалізувати керування ключами, шифрування тощо, для захисту робочих навантажень та інформації. За допомогою сервісів із категорії захисту даних, можна реалізувати наступні параметри:

- *Конфеденційність даних.* Сервіси AWS пропонують широкий функціонал для підтримки конфеденційності даних, використовуючи ресурси для управління конфденційністю, яка включає в себе введення та шифрування журналів, розширений доступ. При чому можна викристовувати ключі та управляти ними, навіть якшо вони були створені за межами хмарного профайдеру AWS.

- *Контроль та розміщеня даних.* Керування даними їх розміщення, захист та розподілення ролей доступу до них, все це можна реалізувати використовуючи сервіси AWS. Найголовніше, що у весь реалізований функціонал відповідає вимогам безпеки та дозволяє не переживати за безпеку в цьому процесі.

- *Захищеність.* Можна використати комплексні послуги безпеки для покращення відповідностей до основних вимог. Крім того є можливість створювати ключі шифрування та керувати ними, при цьому реалізовувати моніторинг та введення журналів, для того аби завжди відповідати вимогам безпеки.

- *Цифровий суверніmет.* Збереження даних клієнтів, наприклад, додатку, можна у всьому світі, відповідно в різних регіонах. При цьому їх безпека залишається на відповідному рівні, а використову.чи набір сервісів доступний контроль та функції цифрового суверніmету для постійної відповідності вимогам.

До сервісів другої категорії можна віднести наступні:

- AWS Certificate Manager – пропонує сертифікати SSL/TLS для підключених ресурсів та сервісів AWS, та реалізовує керування ними.
- AWS Key Management Service (AWS KMS) – використовується для створення ключів та керування ними, для шифрування або ж для цифрових підписів особистих даних.
- AWS Payment Cryptography – допомагає полегшити криптографічні операції в особистих хмарних платіжних додатках, при цьому не нехтуючи безпекою.
- Amazon Macie – захищає конфіденційні дані в будь-якому масштабі.
- AWS Secrets Manager – використовується для централізованого управління життєвого циклу секретів.
- AWS CloudHSM – допомагає керувати однокористувацькими апаратними модулями безпеки.

- AWS Private Certificate Authority – створює приватні сертифікати для захисту даних та ідентифікації ресурсів.

3. Керування ідентифікацією та доступом. Основними принципами безпеки для будь-якої організації є контроль доступу та управління ідентифікацією. Сервіси AWS пропонують можливості ідентифікації в додатках для користувачів та робочих навантажень, що дозволяє швидко приступити до роботи з даним функціоналом. Безпечне управління ресурсами, доступом тощо, можливе у будь-якому масштабі. Для забезпечення безпеки, використання даних сервісів допомагає реалізувати наступні дії:

- *Детальне управління доступом та аналіз.* Використовуючи ресурси для управління доступом на основі правил та атрибутів у будь-якому масштабі, допомагає розробити для клієнтів детальний доступ до ресурсів, робочих навантажень та додатків, що в подальшому підвищує рівень безпеки.

- *Масштабовані рішення по ідентифікації користувачів та співробітників сервісу.* Реалізація безпечного та у будь-якому масштабі керування ідентифікаційними даними, дозволами та доступами до ресурсів, відбувається за рахунок сервісів ідентифікації, які мають високий рівень доступності та є відмовостійкими.

- *Управління ідентифікаційними даними та доступом.* Використовуючи автоматизацію та централізацію керування доступом, виникає можливість для покращення продуктивності та ефективності, та додатково забезпечити безперебійний контроль.

До сервісів третьої категорії можна віднести наступні:

- Amazon Verified Permissions – реалізовує керування конкретними дозволами та авторизацією в користувацьких додатках.

- AWS IAM Identity Center (successor to SSO) – централізоване керування доступом співробітників до комерційного додатка та безлічі акаунтів AWS.

- AWS Organizations – централізоване управління робочого середовища в міру масштабування ресурсів.

- Amazon Cognito – реалізація надійної та простої ідентифікації користувачів з масштабованим керуванням доступу.
- AWS Resource Access Manager – легкий та безпечний обмін власними ресурсами AWS з іншими обліковими записами користувачів.
- AWS Identity and Access Management (IAM) – безпечне керування доступом до ресурсів та сервісів, та управління ідентифікаційними даними.
- AWS Directory Service – повністю керований сервіс Microsoft Active Directory.

4. Захист мережі та додатків. додатків надають можливості застосування політик безпеки у точках контролю мережі в рамках підприємств тощо. Тому в подальшому можна не тільки фільтрувати трафік, а й перевіряти його, для того аби не виникало несанкціонованого доступу на рівні границь мережі, хосту і застосунків. Використання сервісів для захисту мережі та додатків, реалізовує наступні заходи безпеки:

- *Активний захист від широкого діапазону ризиків.* Використовуючи широкий асортимент сервісів для забезпечення захисту мережі, можна реалізувати оперативний контроль трафіку для забезпечення від несанкціонованого доступу, зниження продуктивності, потенційних вразливостей, крадіжки інформації тощо.

- *Перевірка в масштабі.* Завдяки захищеним мережам та додаткам, можна автоматично масштабувати механізми перевірок та захисту, для забезпечення високої доступності робочих навантажень, при цьому без необхідності керування інфраструктурою.

- *Централізоване керування.* За допомогою сервісів даної категорії, можна виконувати централізоване керування правилами брандмауера для особистих акаунтів, при чому виконувати агреговані звіти про забезпечення коректних вимог політики у створеній хмарній інфраструктурі.

- *Видимість трафіку у широкому спектрі.* Забезпечення видимості трафіку в режимі реального часу, в незалежності від портів, або ж протоколу,

за допомогою якого можна включати детальний моніторинг, ведення журналів та фільтрацію.

До сервісів четвертої категорії можна віднести наступні:

- AWS Shield – використовується для управління захистом від DDoS атак, що допомагає максимізувати доступність та швидкість реагування додатків у разі небезпек.
- AWS Firewall Manager – реалізовує централізоване налаштування правил брандмауерів та керування ними для всіх власних акаунтів.
- Amazon Route 53 Resolver DNS Firewall – фільтрує та контролює вихідний DNS – трафік для власних VPC.
- AWS Verified Access – забезпечення доступу до корпоративних додатків без VPN.
- AWS Network Firewall – резервування мережі міжмережного екрана на власних VPC.
- AWS Web Application Firewall (WAF) – захист власних веб-додатків від найвідоміших експлойтів.

5. Схвалення вимог. Можна використовувати комплексні представлення про стан відповідності вимогам та постійно контролювати власну інфраструктуру за допомогою автоматизованих перевірок відповідності на основі найкращих практик безпеки та відповідних стандартів, які будуть відповідати вимогам додатка, організації тощо. Використання сервісів з даної категорії вирішує низку наступних питань:

- *Швидке усунення неполадок.* За рахунок швидкого виявлення не відповідних ресурсів та шляхом швидкої доставки інформації й журналів подій, реалізовується постійна відповідність вимогам. Тому в подальшому можна отримувати уявлення про стан та процеси забезпечення заявленим вимогам, для захисту інфраструктури до появи загроз.

- *Покращення існуючої безпеки.* Налаштування безперервного моніторингу власних ресурсів у будь-якому регіоні та облікових записів,

створення перевірених файлів журналів всіх користувачів, все це покращує безпеку.

- *Збір та аудит даних.* Використовуючи дані сервіси можна скоротити помилки які залежать від людського фактора, за допомогою автоматизації збору точної інформації, яка заздалегідь обрана для аудиту. Даний механізм допомагає реалізувати аудит, саме з тих даними, які були обрані заздалегідь та які не були підробленими.

До сервісів п'ятої категорії відносяться:

- AWS Artifact – це безкоштовний портал для самообслуговування, який забезпечує доступ до потреб звітів про безпеку.
- AWS Audit Manager – використовується при перевірці, для спрощення оцінки ризиків та відповідності до вимог.

2.4 Архітектура інфраструктури хмарного сервісу

Архітектура є невід’ємною частиною розробки більшості проєктів, програмних продуктів тощо. Хмарна інфраструктура не стає винятком з даного переліку. Проєктування архітектури, допомагає візуально відобразити все те, що буде розгортатись та реалізовуватись на подальшому етапі розробки. Іншими словами архітектура хмарної інфраструктури стає шаблоном на основі якого і відбувається подальша розробка.

Для початку визначаються ті частини та механізми які саме будуть реалізовуватись в інтернет-магазині та будуть функціонувати у хмарній інфраструктурі. В даному проєкті буде реалізовано хмарну інфраструктуру на базі AWS із роз'єднаним інтерфейсом користувача та серверною частиною, іншими словами на базі клієнт-серверної архітектури.

Невід’ємною частиною архітектури буде захист та автентифікація користувачів, яка проходить межування із захистом. Необхідно врахувати додаткові можливості комерційного характеру, такі як пошук, сервіси визначення місцезнаходження тощо.

Після того як структура архітектури більш менш визначена, необхідно підібрати найоптимальніші сервіси, які будуть реалізовувати функціонал кожної частини. Звичайно, що в майбутньому цей список буде тільки розширятись. Розроблена архітектура представлена на рисунку 2.4.1, а детальний опис архітектури продовжується далі.

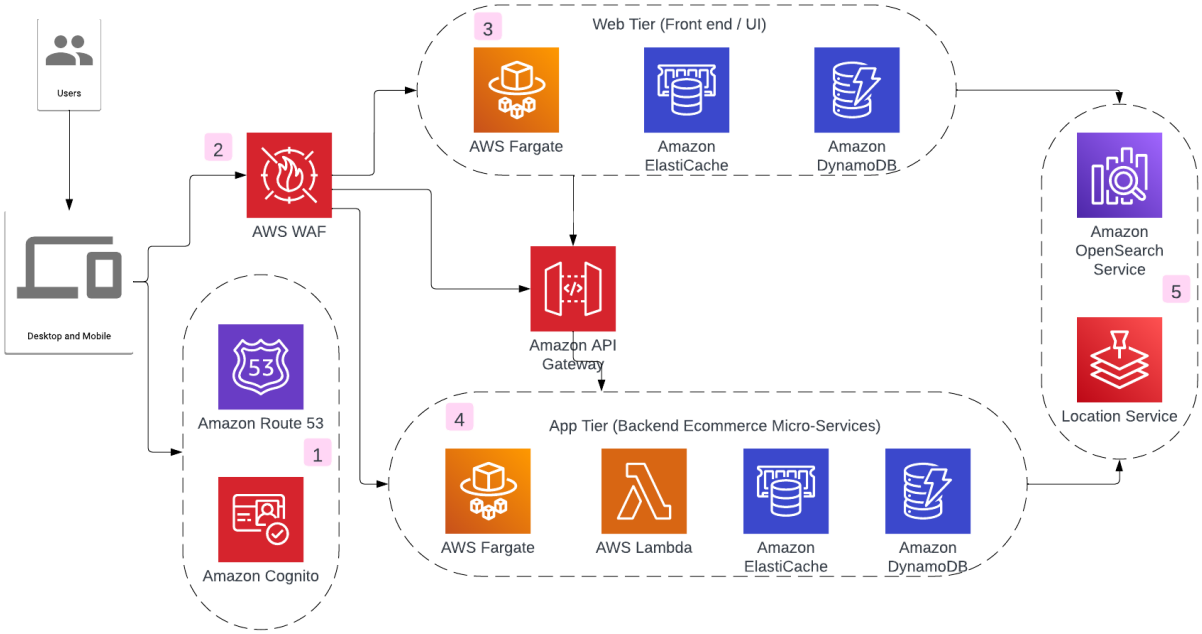

Рисунок 2.4.1 – Архітектура хмарної інфраструткутри

Під цифрою 1 на рисунку 2.4.1 представлено сервіс AWS Cognito та Amazon Route 53, які будуть розгортатись та більш детально розглядатись далі, у частині аутентифікації клієнтів та методів доступу до веб-застосунку. Далі архітектура включає елемент захисту, який зображений під цифрою 2 на рисунку 2.4.1 та представлені усі подальші зв'язки з іншими елементами. Під цифрою 3 розглядається низка сервісів, які формують собою клієнтську частину сервісу, а під цифрою 4 серверна частина сервісу, які взаємодіють також через запити та відповіді API. Останньою частиною архітектури є комерційна, яка базується під цифрою 5 на рисунку 2.4.1.

В подальшому дана архітектура при розробці може змінюватись в залежності від додавання нових сервісів, можливостей, або ж відмови від тих сервісів, які вже є в архітектурі. Але на даному етапі архітектура є доцільною

та буде розгортатись та обґрунтовуватись вибір сервісів для даної інфраструктури в наступному розділі, тобто 3.

2.5 UML- моделі хмарного сервісу

UML- діаграми є популярними та зручними при будь-якій розробці, будь то програмне забезпечення, хмарна інфраструктура, веб-додаток тощо. Існує 12 різновидів UML- діаграм, які в залежності від типу можуть представляти фізичні аспекти функціональності продукту, поведінкові, або ж якусь статичну структуру. Кожен розробник обирає сам, що саме він бажає представити у власному проєкті. Оскільки не всі діаграми є доцільними саме для даного проєкту, або ж якогось іншого, тобто вибір випливає зі специфіки розробки і т.д.

Доцільно розробити діаграму прецедентів (use-case diagram). Починати краще з аналізу функціонала хмарної інфраструктури, наприклад, з рисунка 2.4.1, та вимог, які вказані у технічному завдані. Під час аналізу визначають зовнішніх користувачів для хмарної інфраструктури та перелік аспектів властивих поведінці такого користувача у процесі взаємодії з інфраструктурою. Такі аспекти поведінки хмарної інфраструктури й будуть прецедентами, які є одним з елементів даної діаграми.

Діаграма прецедентів допоможе візуально представити очікувану поведінку системи. Вона складається з двох елементів, один це прецеденти, а інший учасник, якого визначають під час аналізу та які пов’язуються між собою зв’язками. Діаграма прецедентів UML на рисунку 2.5.1.

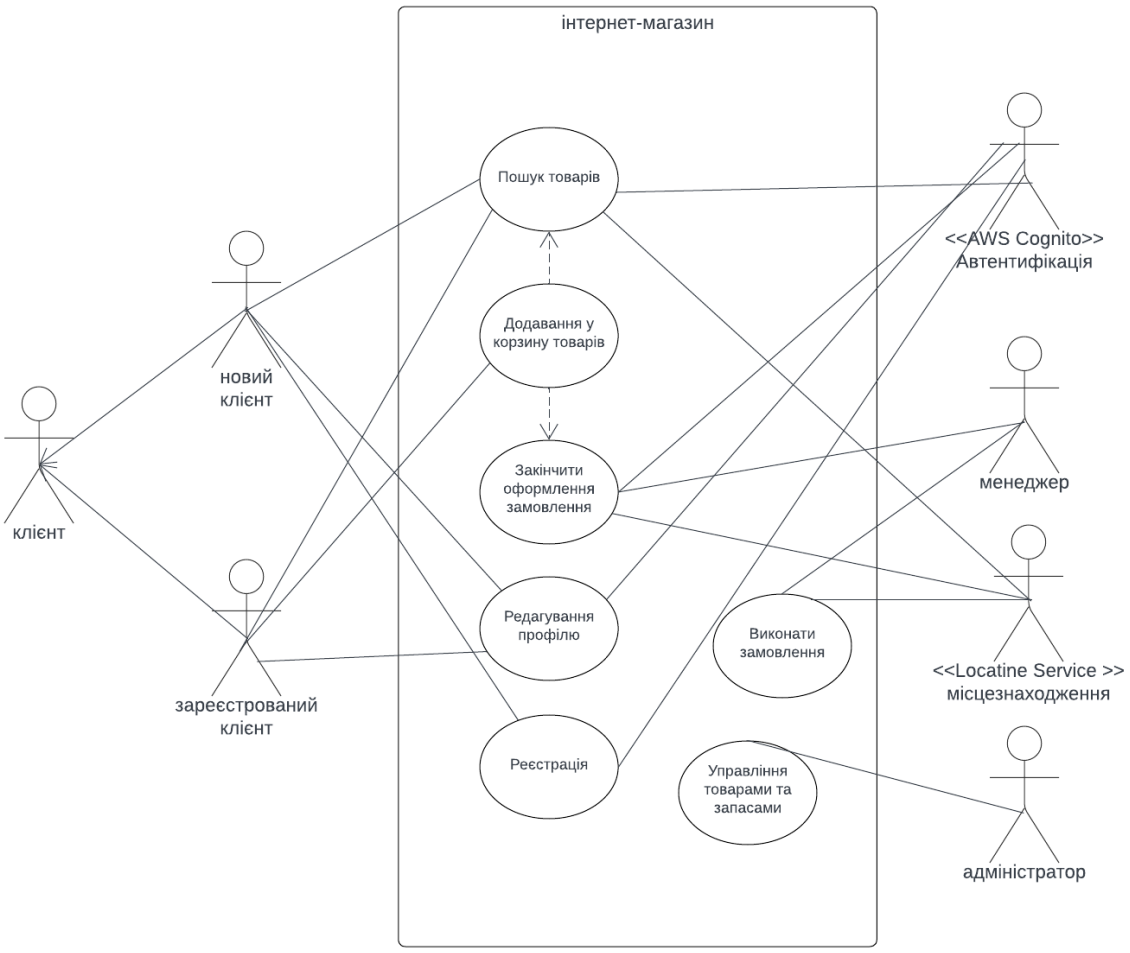

Рисунок 2.5.1 – Діаграма прецедентів

Висновки до розділу 2

У другому розділі створено акаунт у системі AWS та проведено докладний аналіз класифікацій сервісів і їх подальших категорій. Розглянуті сервіси та базові принципи функціонування сервісів із різних класифікацій, які можуть бути реалізовані для різних сфер, а не тільки для сфери комерції. Більш детально представлені сервіси захисту інформації та безпеки в цілому. Розглянуто кожен сервіс із даної галузі та методи застосування і реалізації, так як безпека є важливою складовою.

Другий розділ вмістив розробку архітектури хмарної інфраструктури для інтернет-магазину з підбором сервісів, які будуть реалізовуватись та розгортатись у наступному розділі. Розроблена UML-діаграма прецедентів для хмарної інфраструктури.

РОЗДІЛ 3. Реалізація інфраструктури хмарного сервісу

3.1 Розгортання аутентифікації клієнтів та методів доступу до веб-додатку

Більшість систем які реалізовуються сьогодні, мають різноманітні способи для аутентифікації користувачів. В першу чергу авторизацію користувачів звичайно реалізовують саме для безпеки, будь то витік даних, чи отримання доступу до конфіденційної інформації і т.д.

Процес авторизації включає в себе як ідентифікацію, так і аутентифікацію. Реалізація ідентифікації може бути різна, в залежності від потреб, найчастіше це електронна адреса, або ж номер телефону, але можуть бути й інші методи. Аутентифікація в подальшому, являє собою підтвердження, того, що ви насправді являєтесь тим, за кого себе видаєте, тобто ідентифікуєте. Аутентифікація буває також різна, це може бути пароль, сертифікат тощо. Після проходження цих етапів настає процес авторизації, в якому вже перевіряється уся інформація та робиться висновок, чи отримається доступ.

Оскільки розроблена архітектура хмарного сервісу, яка зображена на рисунку 2.1.3, реалізується на AWS, то для реалізації процесу аутентифікації клієнтів та методів доступу до веб-додатку, доцільно обрати сервіс ***Amazon Cognito.*** Звичайно існують аналоги даного сервісу такі як Google Cloud Identity Platform, Azure Active Directory B2C, IBM Security Verify тощо, але в інших хмарних провайдерів, тому вони не розглядаються більш детально.

Amazon Cognito дозволяє швидко та без ускладнень реєструвати користувачів та виконувати вхід у систему, та авторизувати серверні API. Однією з переваг даного сервісу є масштабування до мільйона користувачів та підтримка входу в систему з різними постачальниками соціальних ідентифікаторів (Google, Amazon тощо).

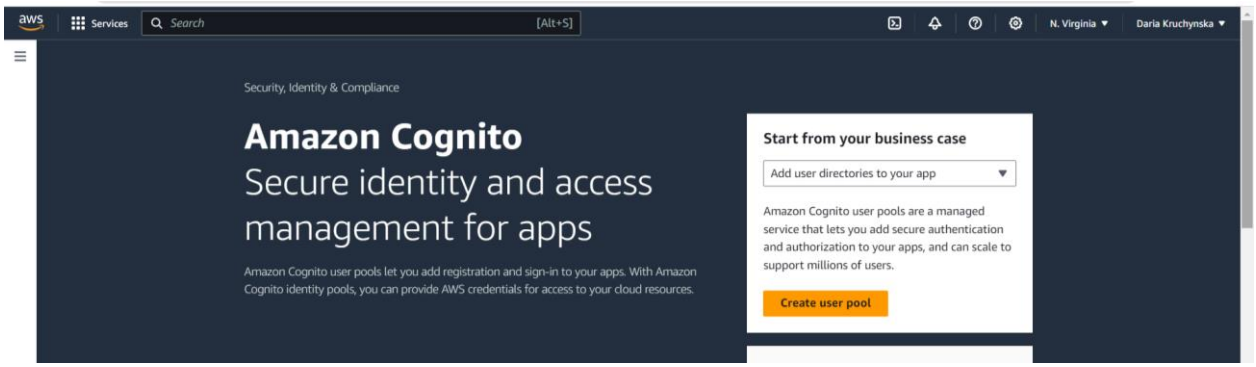

Рисунок 3.1.1 – Створення пулу користувачів за допомогою сервісу Amazon Cognito

Для створення пулу користувачів необхідно нажати відповідну кнопку “Create user pool”, яка зображена на рисунку 3.1.1. Створення пулу користувачів складається з 7 етапів. ***На першому етапі*** налаштовується вхід у систему. Вирішується чи використовувати тільки свій власний новий пул користувачів, який буде окремим каталогом користувачів, або ж додатково інтегрувати його з об’єднаними постачальниками ідентичності.

Сервіс Amazon Cognito дозволяє використовувати ідентифікаційні дані таких постачальників Facebook, Apple, Amazon тощо. Для налаштування власного пулу користувачів для управління авторизацією можна обрати потрібні варіанти ідентифікації користувачів з каталогу Amazon Cognito, такі як електронна пошта, унікальне ім’я (яке вводить користувач сам для себе) або ж номер телефону.

У власному проєкті за замовчування обрано створення власного пулу та додатково налаштування пулу користувачів який буде інтегруватись з об’єднаними постачальниками ідентичності, реалізація показана на рисунку 3.1.2.

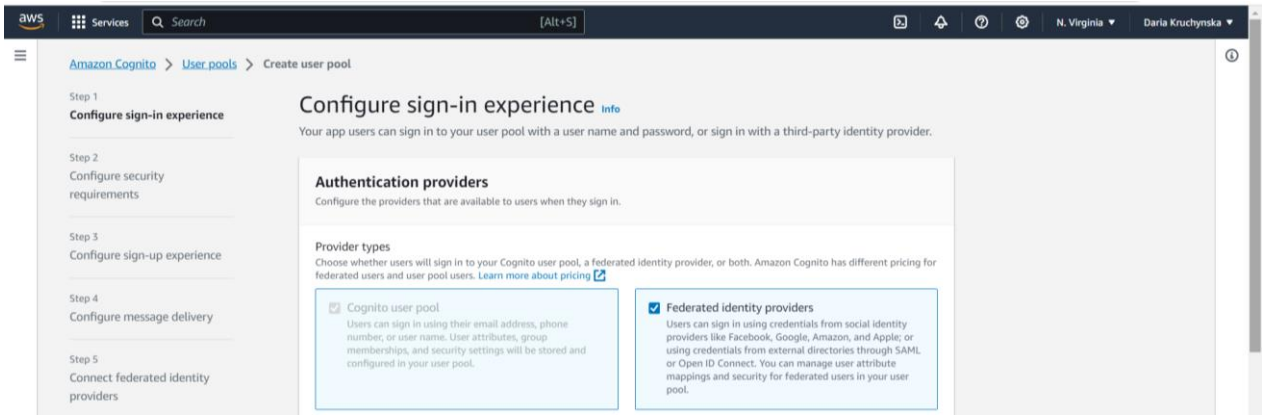

Рисунок 3.1.2 – Обрання типів аутентифікації для входу у систему

Після того як тип аутентифікації обраний, необхідно визначити додаткові параметри, за якими буде відбуватись аутентифікація для обох варіантів. Для варіанту з власним пулом обрано аутентифікацію за електронною адресою та номером телефону тому, що з особистого досвіду та аналізу інформації, аутентифікація за унікальним ім’ям не така зручна.

Для другого варіанту аутентифікації обрано таких постачальників ідентичності як Facebook, Apple та Google. Даний вибір є більш доцільним для нашої місцевості та для самого додатку. Якщо додаток буде масштабуватись у регіональному значені, то звичайно цей список можна буде розширити, це все можна побачити на рисунку 3.1.3.

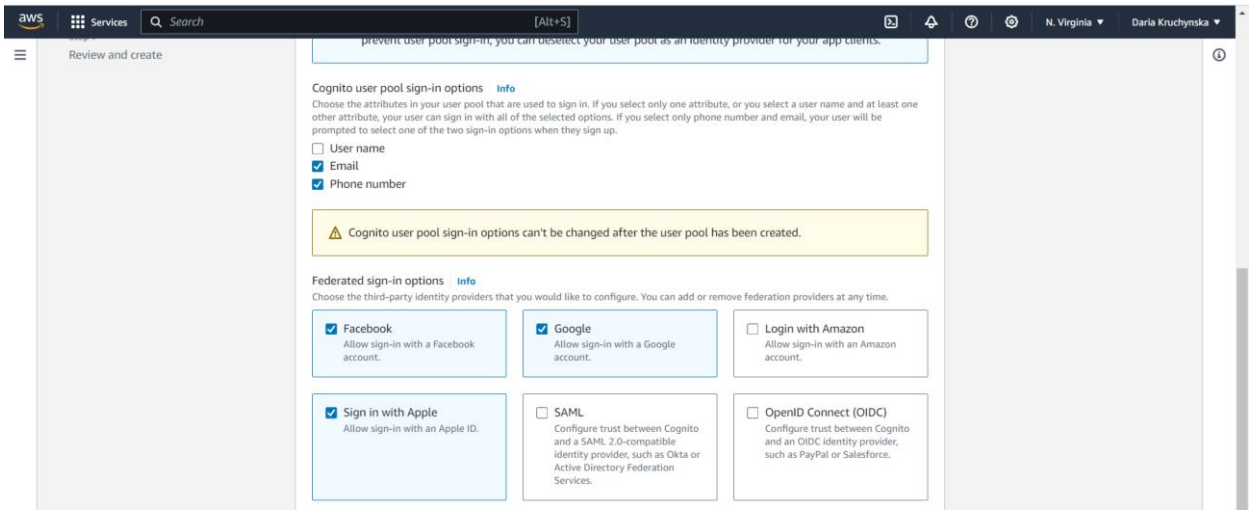

Рисунок 3.1.3 – Обрання параметрів для обох типів аутентифікації

На другому етапі створення пулу користувачів, налаштовується політика безпеки аутентифікації користувачів. Amazon Cognito має можливості для

підвищення безпеки входу у систему, а також для коректного відновлення паролів, для користувачів, у випадку втрати пароля.

У першу чергу налаштовується політика паролів на рисунку 3.1.4, можна обрати налаштування за замовчуванням, або ж власні. Обрано налаштування власної політики, адже аналізуючи останню інформацію на сьогодні, більшість рекомендацій, стосовно мінімальної довжини пароля, становить вже не 8 символів, а від 10-12. Саме тому доцільно змінити значення мінімального пароля за замовчуванням, а всі інші політики залишаються незмінними, так як є актуальними.

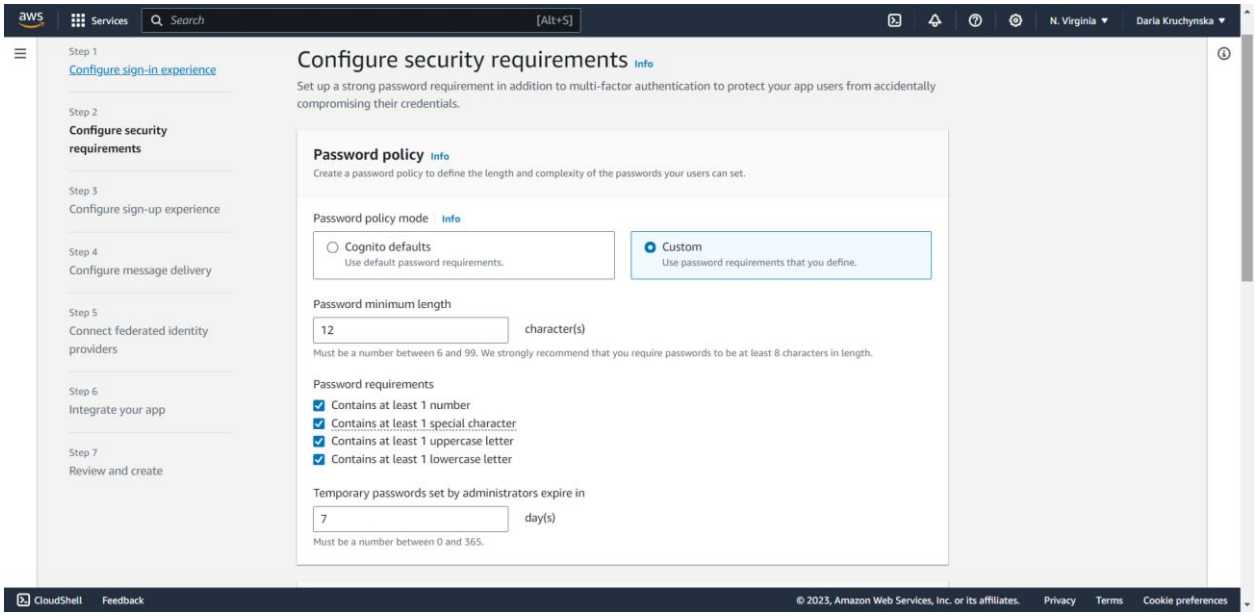

Рисунок 3.1.4 – Налаштування політики паролів

Наступним параметром налаштування політики аутентифікації є встановлення параметрів для багатофакторної аутентифікації (MFA), реалізованої на рисунку 3.1.5. Обрано обов'язкову багатофакторну аутентифікацію з методом через додаток аутентифікації, що є досить зручним та популярним. У майбутньому можна додати додатково аутентифікацію за допомогою SMS-повідомлень. Через те, що ця функція потребує додаткових витрат, тому у даному проєкті вона є недоцільною.

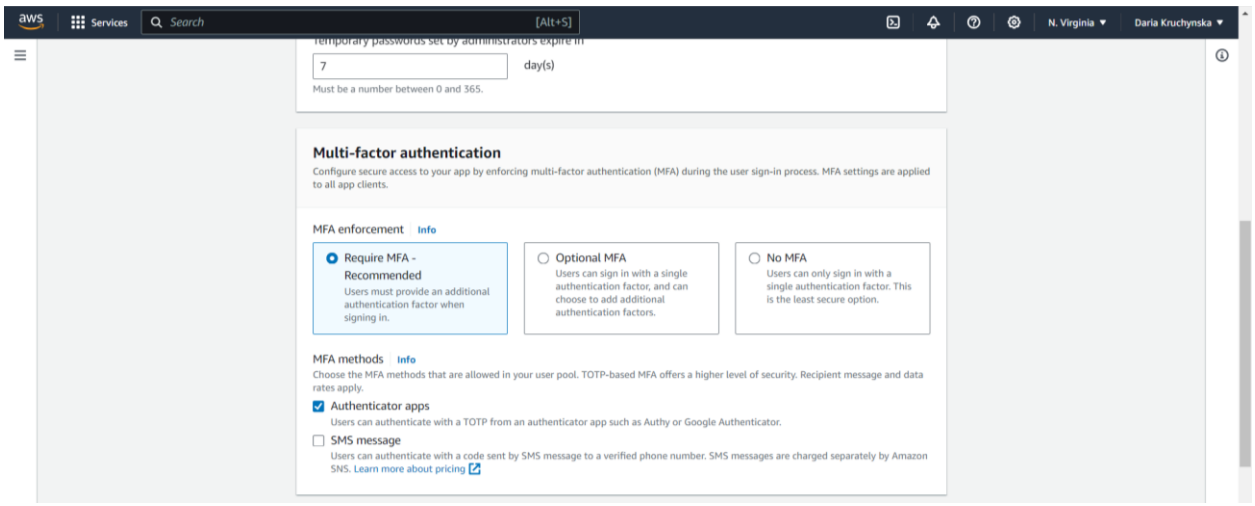

Рисунок 3.1.5 – Налаштування багатофакторної аутентифікації

Наступний крок налаштування параметрів для відновлення облікових записів, при втраті пароля, показані на рисунку 3.1.6. Налаштовано самостійне відновлення користувачем, оскільки в іншому випадку потрібно відновлювати адміністратору, за допомогою Cognito API, що на даному етапі є недоцільним. Метод відновлення обраний за допомогою електронної адреси, в іншому випадку через смс.

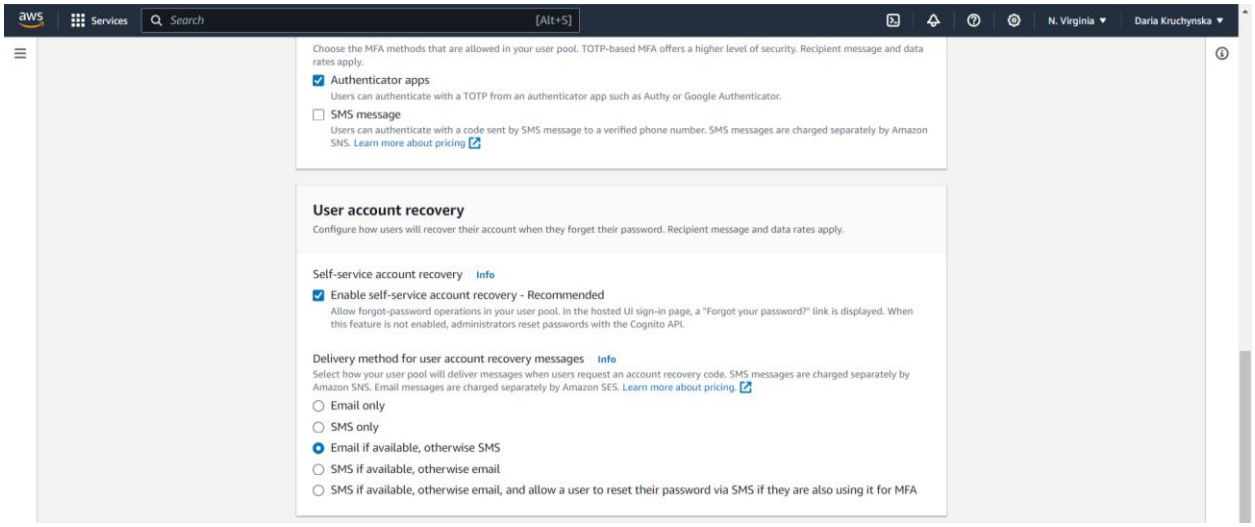

Рисунок 3.1.6 – Налаштування параметрів для відновлення облікових записів

Третій етап створення пулу користувачів полягає в налаштуванні реєстрації нових облікових записів та параметрів авторизації в подальшому. Налаштування параметрів реєстрації, реалізовується на рисунку 3.1.7, обрано самореєстрацію облікових записів, так як це є набагато зручніше. У іншому випадку, необхідно мати додаткового співробітника, або ж бути самому

адміністратором, що є більш затратно та з перспективою на масштабування недоцільним.

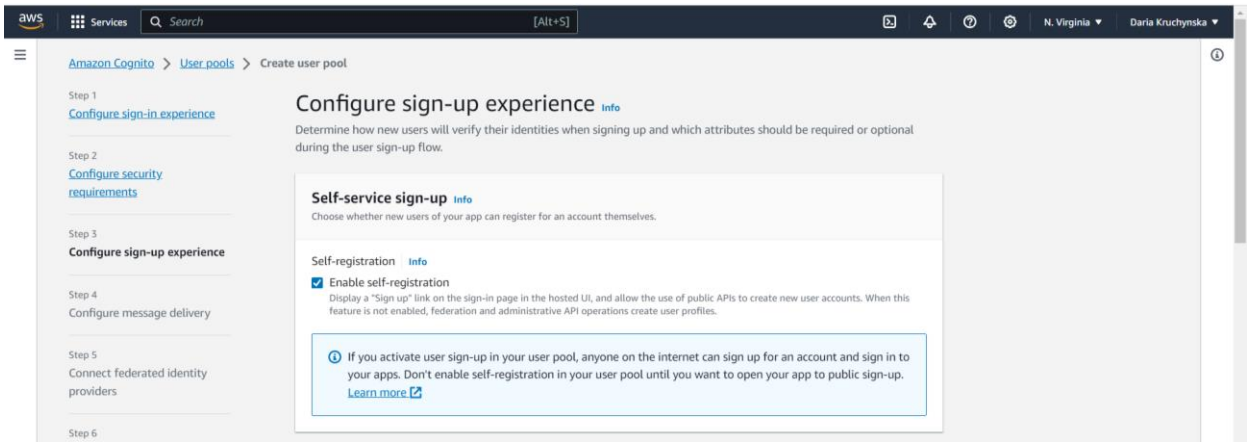

Рисунок 3.1.7 – Налаштування параметрів реєстрації

Далі налаштовуються перевірка атрибутів та підтвердження облікового запису, яка показана на рисунку 3.1.8. Перевірка відбувається використовуючи електронну пошту.

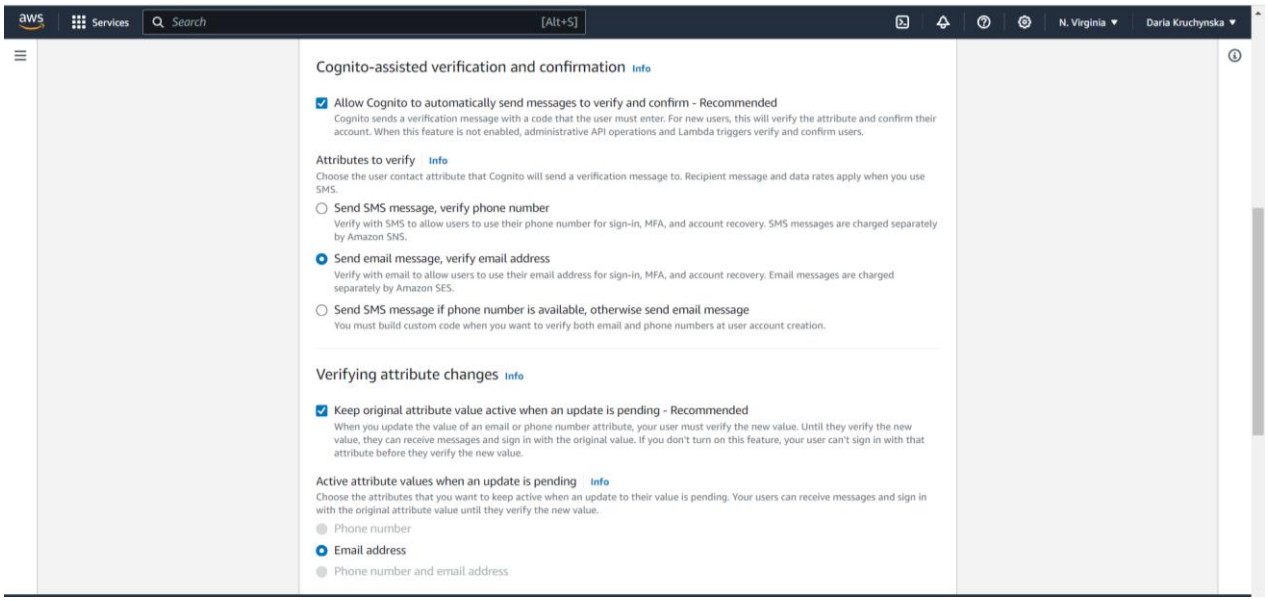

Рисунок 3.1.8 – Налаштування параметрів перевірки атрибутів та верифікації акаунту

Далі необхідно обрати обов’язкові параметри для заповнення користувачем при реєстрації. Обрані параметри показані на рисунку 3.1.9, є наступними: електронна адреса, ім’я, прізвище, номер телефону, дата народження та місцезнаходження.

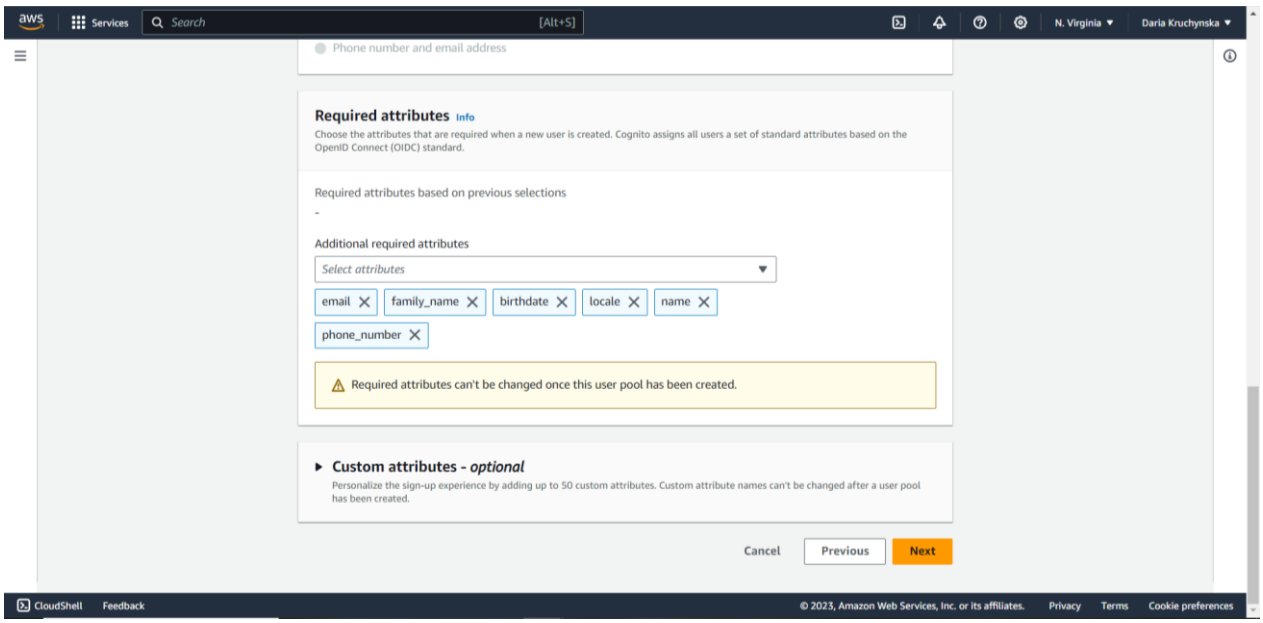

Рисунок 3.1.9 – Налаштування обов'язкових параметрів при реєстрації

Також додатково можна налаштувати спеціалізовані атрибути для персоналізації реєстрації, але це за бажанням. На даний час це не є актуальним для реалізації у проєкті.

На четвертому етапі налаштовується доставлення повідомлень, які будуть надсилатись сервісом Amazon Cognito користувачам при реєстрації, багатофакторній аутентифікації та відновлені облікових записів, а в подальшому інтегруватись від Amazon Cognito до особистого акаунту AWS. Налаштування продемонстровані на рисунках 3.1.10 та 3.1.11, обрано варіанти надсилання повідомлень через електронну адресу Cognito, так як це є доцільним для початкових розробок та дозволяє надсилати до 50 електронних листів на день. Звичайно в подальшому, для продуктивності краще обирати доставляння повідомлень Amazon SES і Amazon SNS, які інтегровані з Amazon Cognito, але це збільшать витрати.

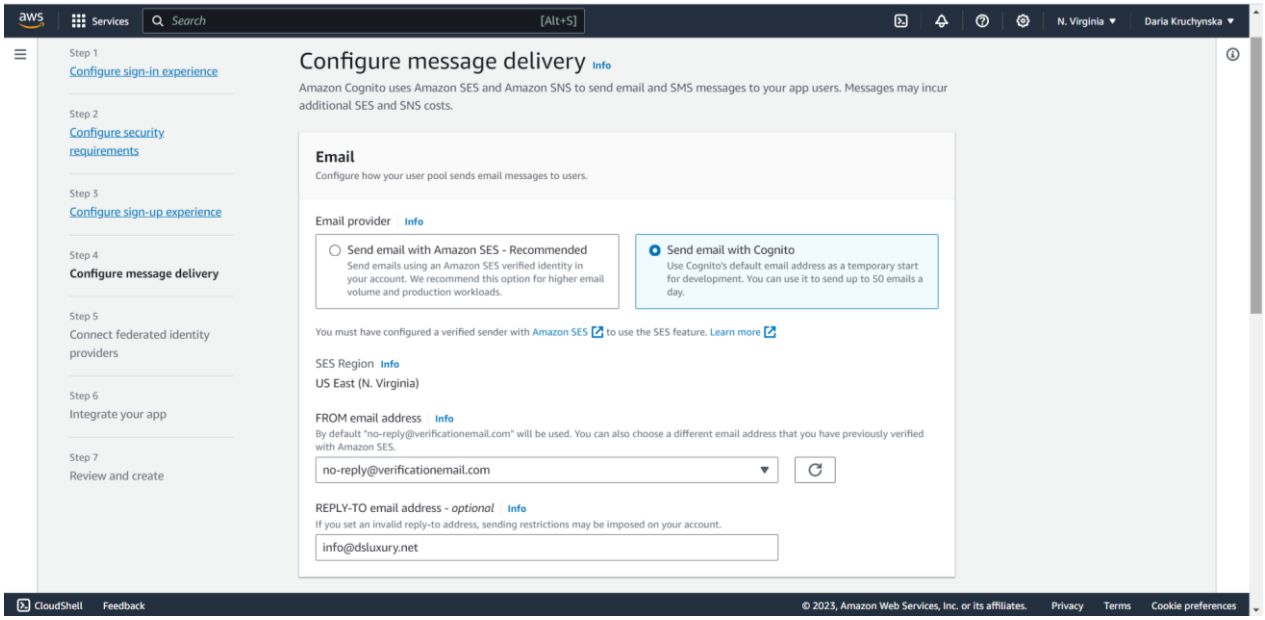

Рисунок 3.1.10 – Налаштування електронних адрес для доставлення повідомлень

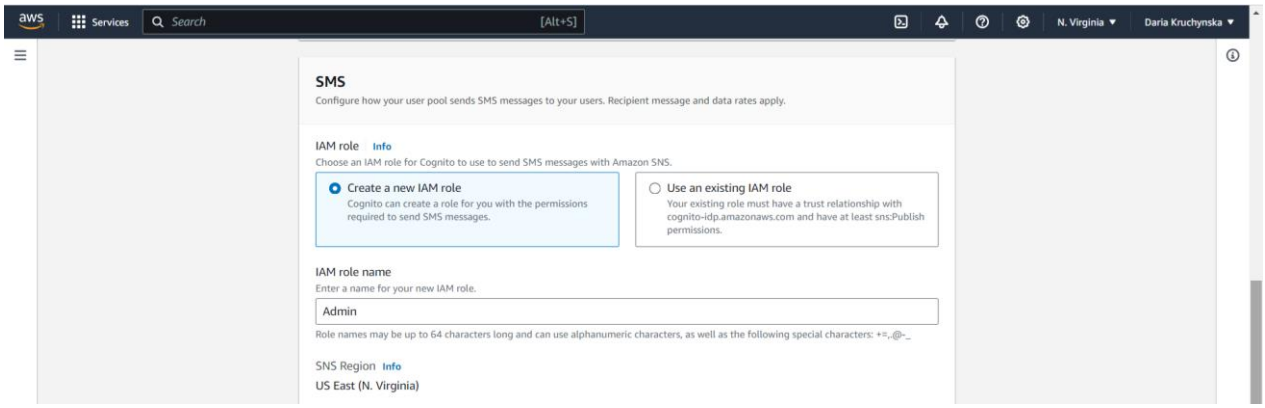

Рисунок 3.1.11 – Налаштування доставлення повідомлень

П’ятий етап налаштовується при подальшій розробці, на цей момент це не є обов’язково. Далі буде налаштована автентифікація за допомогою об’єднаних постачальників, які були обрані на першому етапі та показані на рисунку 3.1.3. На даному етапі налаштовуються зіставлення атрибутів між постачальником та самим сервісом Cognito.

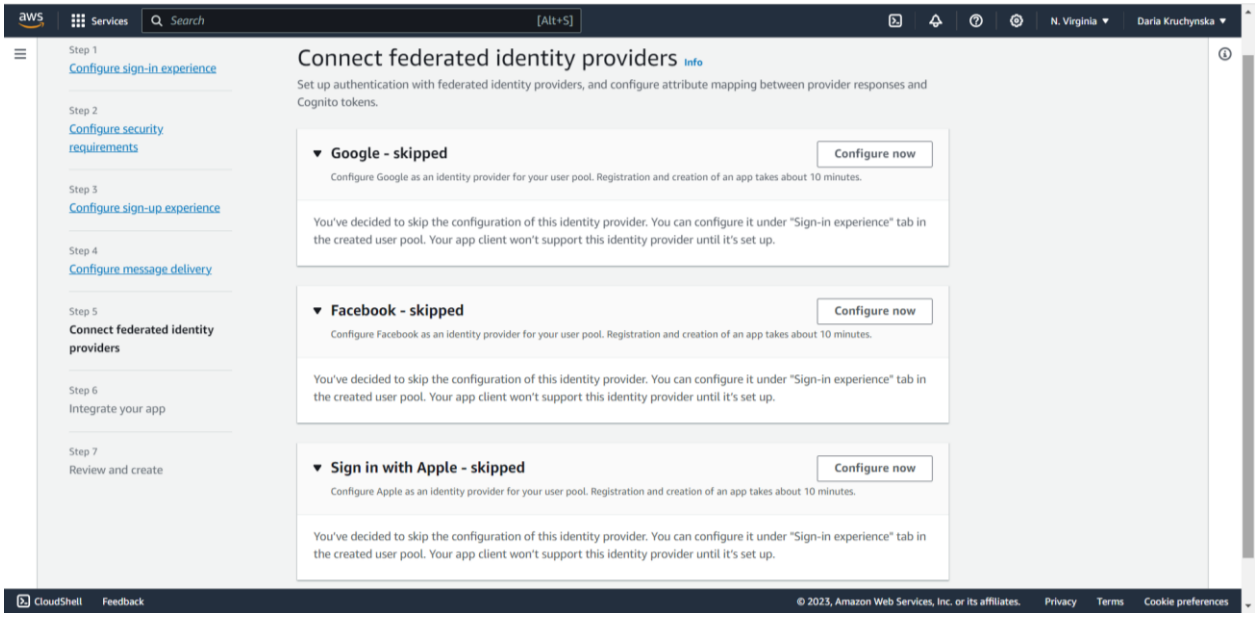

Рисунок 3.1.12 – П’ятий етап створення пулу користувачів

На шостому етапі необхідно інтегрувати інформацію про додаток потрібну для пулу користувачів. Так як на першому етапі були обрані постачальники, які зображені також на рисунку 3.1.3, за допомогою яких будуть автентифікуватись користувачі, тому тепер необхідно налаштувати для них деталі, які потрібні для подальшого встановлення довірчих відносин із постачальниками. Спочатку необхідно дати назву пулу користувачів, яка зображена на рисунку 3.1.13.

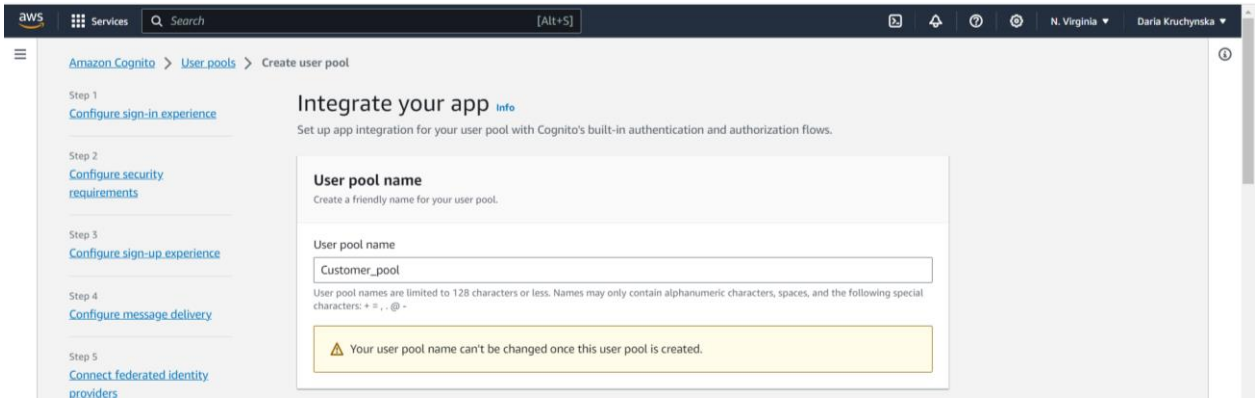

Рисунок 3.1.13 – Назва пулу користувачів

Далі на рисунку 3.1.14 відображається заповнена інформація про домен, де будуть створені кінцеві точки автентифікації та для використання розміщеного інтерфейсу користувача.

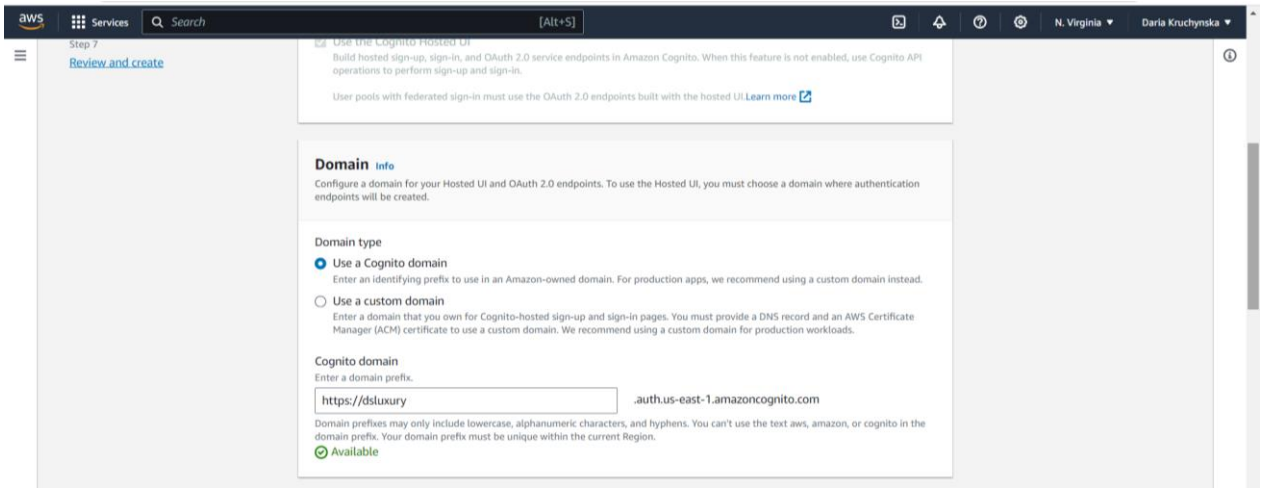

Рисунок 3.1.14 – Заповнена інформація про домен

І останнім є налаштування початкового користувача додатка, який матиме дозвіл на виклик неавтентифікованих операцій API, всі налаштування продемонстровані на рисунку 3.1.15 та 3.1.16.

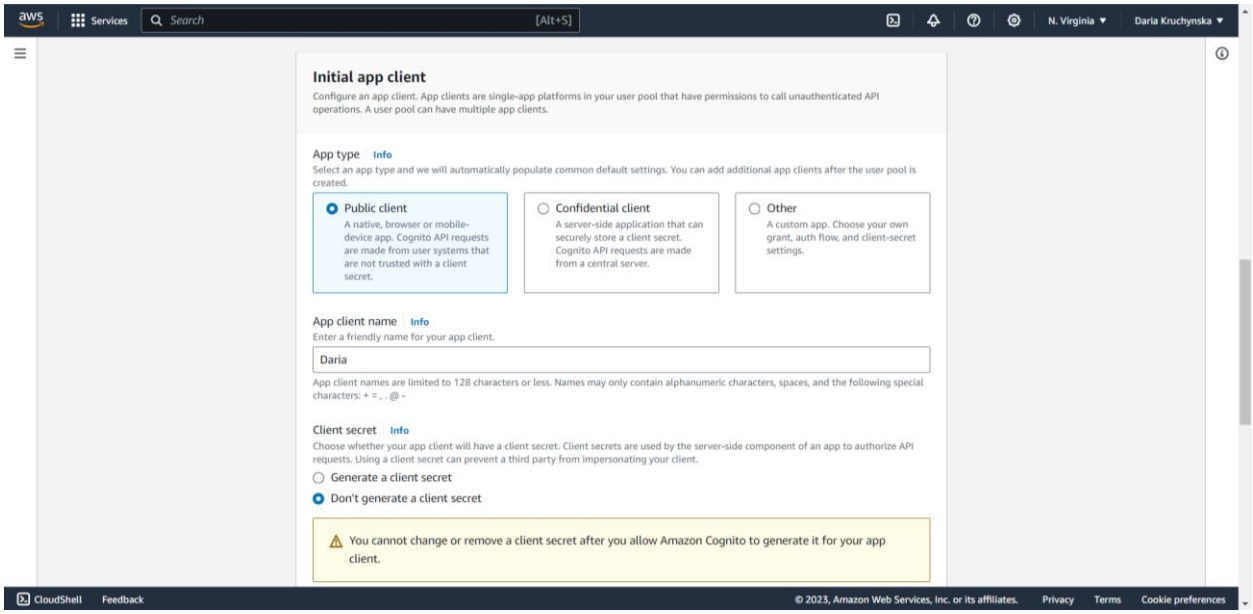

Рисунок 3.1.15 – Налаштування початкового клієнта додатка

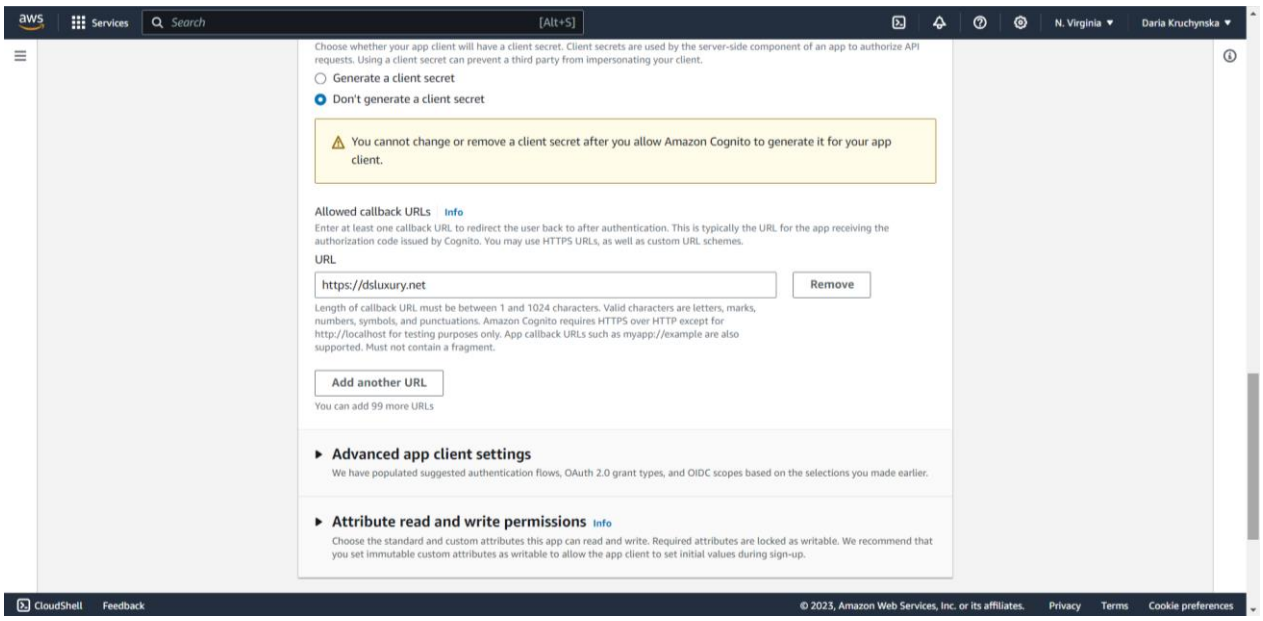

Рисунок 3.1.16 – Додавання URL-адреси зворотного виклику після реєстрації

Останній сьомий етап є завершальним на якому відбувається перевірка усіх налаштувань зроблених на попередніх кроках яке відображено на рисунку 3.1.17.

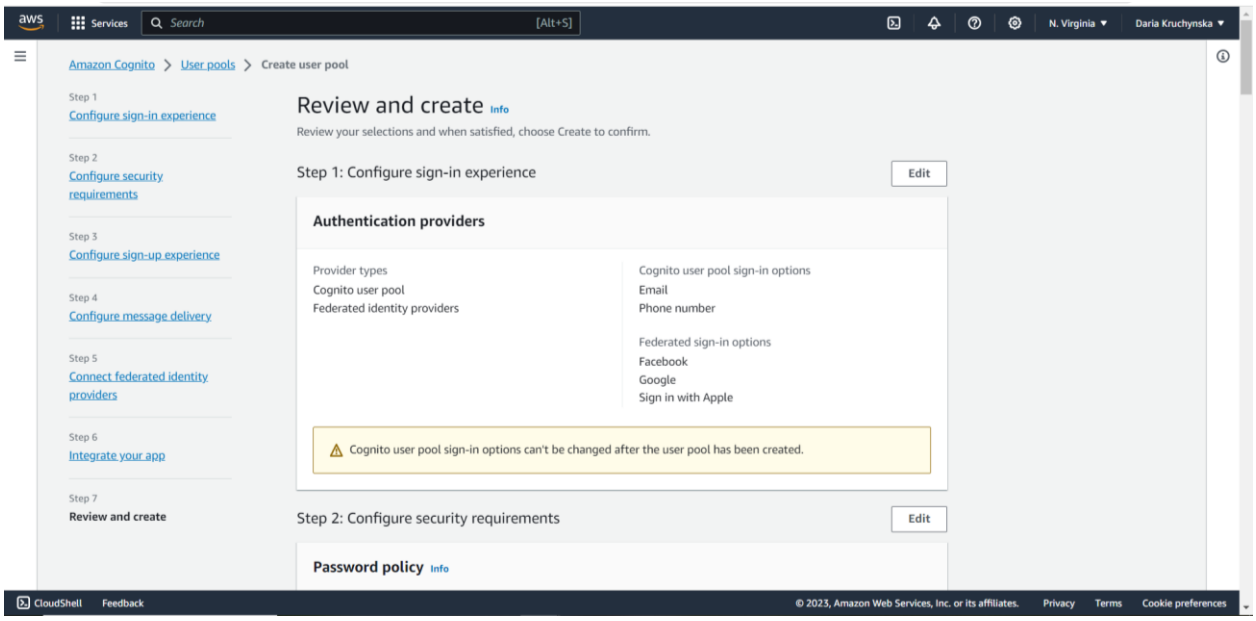

Рисунок 3.1.17 – Перевірка та створення пулу користувачів

Після перевірки усіх етапів, якщо не виникає проблем чи помилок створюється пул користувачів, який відображено на рисунку 3.1.18.

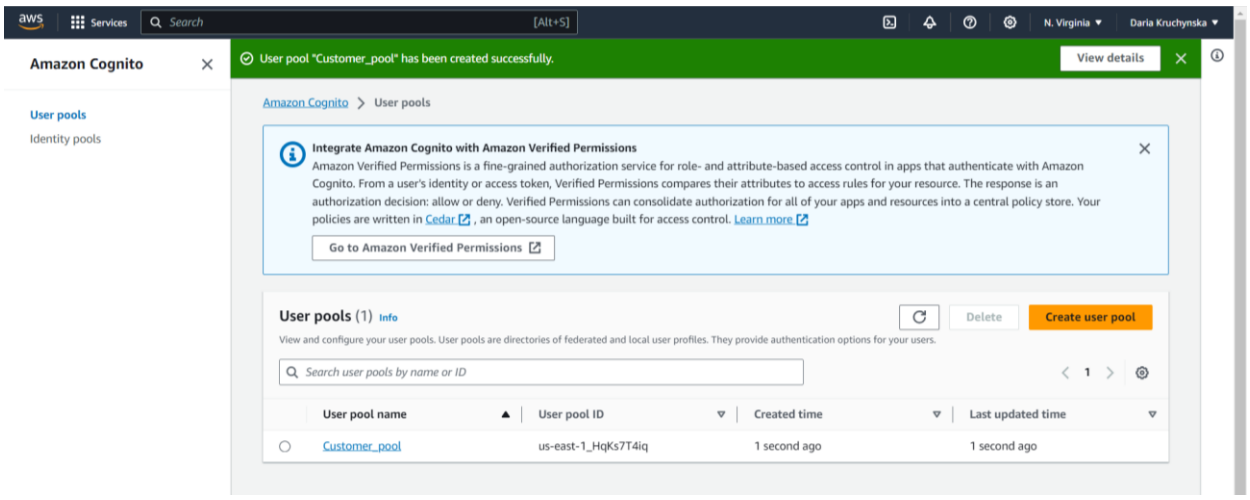

Рисунок 3.1.18 – Успішно створений пул користувачів

Далі необхідно розгорнути наступний сервіс ***Amazon Route 53,*** для того аби клієнти мали можливість отримувати доступ до веб-додатку. Даний сервіс являє собою систему доменних імен (DNS), яка дозволяє зовнішнім клієнтам розпізнавати ім'я веб-сайту та доправляти їх на нього. Це економічний та надійний варіант перенаправлення користувачів до самого веб-додатку.

Amazon Route 53 використовується для з'єднання запитів користувачів із самим веб-застосунком, який розгорнутий в AWS, або ж на локальному сервісі. На рисунку 3.1.19 зображено модель роботи даного сервісу, а саме як реалізовуються DNS – запити користувачами, які розпочинаються з ліва на право по схемі.

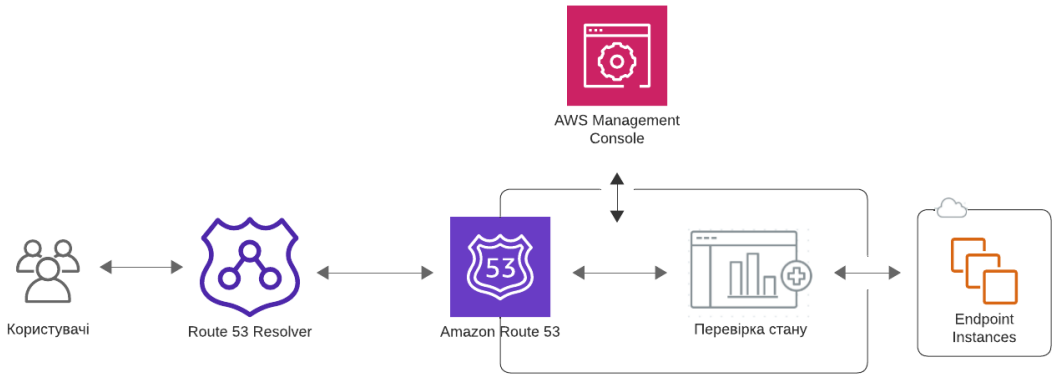

Рисунок 3.1.19 – Принцип роботи сервісу Amazon Route 53

Починається DNS – запит від користувачів та переходить до Route 53 Resolver, іншими словами це порівнювач, або ж радар, який дозволяє запити доменних імен саме від користувачів. Далі на наступному кроці Amazon Route

53, який виступає як авторитетний DNS сервіс, саме він робить повернення ip–адрес для записів DNS, які перед цим запитував Route 53 Resolver. Наступний крок – перевірка стану, яка зображена як гістограма на схемі, на даному етапі відбувається контроль стану особистих кінцевих точок. Даний процес відбувається для забезпечення високого рівня доступності даних точок та відмовостійкості.

Також з самого верху схеми знаходиться AWS Management Console, завдання якого надавати інтерфейс користувачам для створення визначеної зони, правил передавання інформації та відправлення записів DNS у глобальну мережу авторитетних DNS-серверів Route 53. І кінцевою точкою виступають Endpoint Instances, які є кінцевими точками, тобто це три комп'ютери, які знаходяться у хмарі.

Далі нам необхідно зареєструвати доменне ім'я, використовуючи сервіс Amazon Route 53, за допомогою якого у майбутньому буде отримуватись доступу до конкретного інтернет – магазину, який буде розгорнутий у створеній хмарній інфраструктурі. Для початку роботи даного сервісу необхідно натиснути відповідну кнопку "Get Started with Amazon Route 53" як на рисунку 3.1.20.

Рисунок 3.1.20 – Початок роботи з сервісом Amazon Route 53

Для початку необхідно обрати, що саме необхідно реалізувати за допомогою сервісу Amazon Route 53, як на рисунку 3.1.21, в нашому випадку це реєстрація доменного ім'я, як зазначалось раніше. За допомогою даного сервісу можна не тільки реєструвати доменне ім'я, а й навіть транспортувати

доменне ім’я з будь-якого іншого сервісу, якщо воно вже створене, що є досить зручним.

Також використовуючи даний сервіс, у майбутньому можна створити приватну зону, що позитивно впливає на безпеку хмарної інфраструктури та захищає від таких атак, як наприклад DNS brute-force, за рахунок обмеженого доступу до DNS – записів доменну. Додатково можна виконати налаштування для перевірки стану, потоку трафіку тощо.

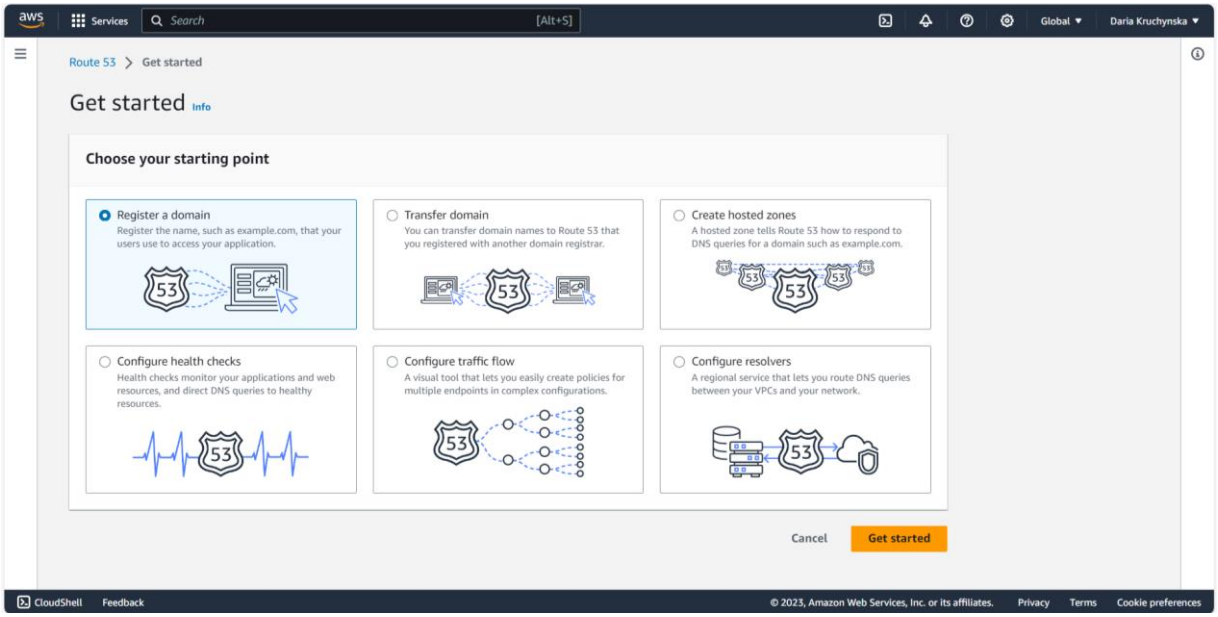

Рисунок 3.1.21 – Вибір функції яка буде реалізовуватись в Amazon Route 53

Після того, як обрано функцію, зареєструвати доменне ім’я на рисунку 3.1.21, починається процес реєстрації, який показаний на рисунку 3.1.22. Спочатку необхідно ввести доменне ім’я, яке необхідно зареєструвати, в нашому випадку *dsluxury.com*. Нажаль дане доменне ім’я вже зайняте, тому сервіс пропонує інші варіанти, яких є 9 та одразу з ціною, тож можна обрати саме той варіант, який потрібно.

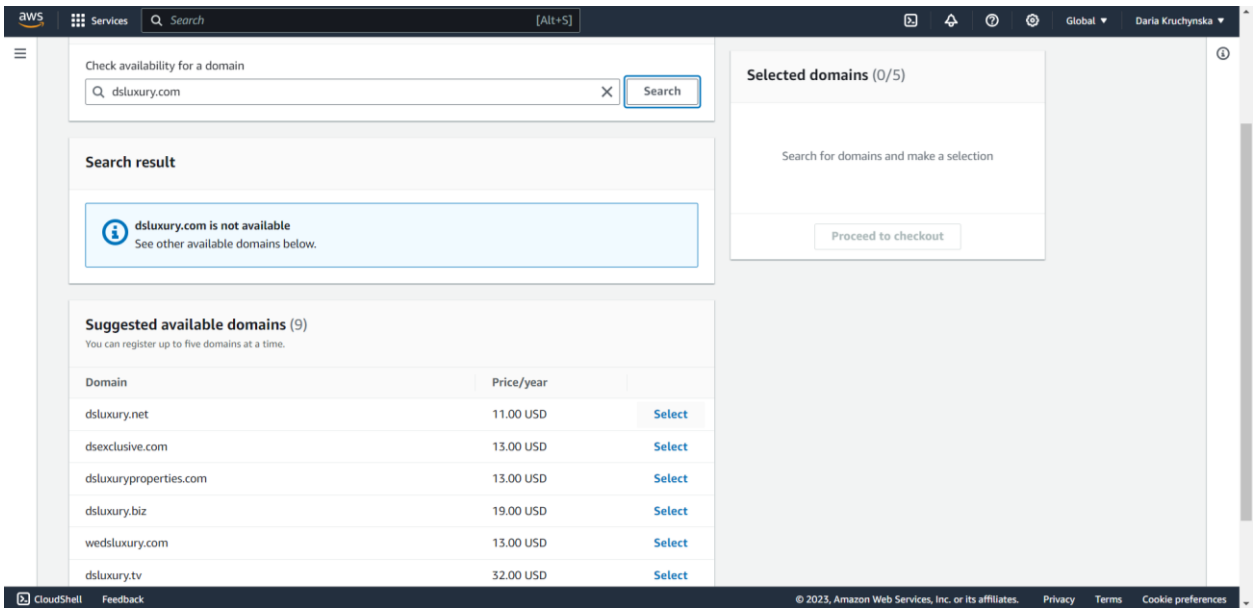

Рисунок 3.1.22 – Початок реєстрації доменного імені

Після того як отримано варіант доменних імен, робиться вибір, як на рисунку 3.1.23. В даному випадку вибір падає на перший варіант, а саме *dsluxury.net*, так як він є найоптимальнішим. Адже дане доменне ім’я має найменшу ціну за рік, лише 11$ та змінюється лише доменна зона, а назва залишається без змін.

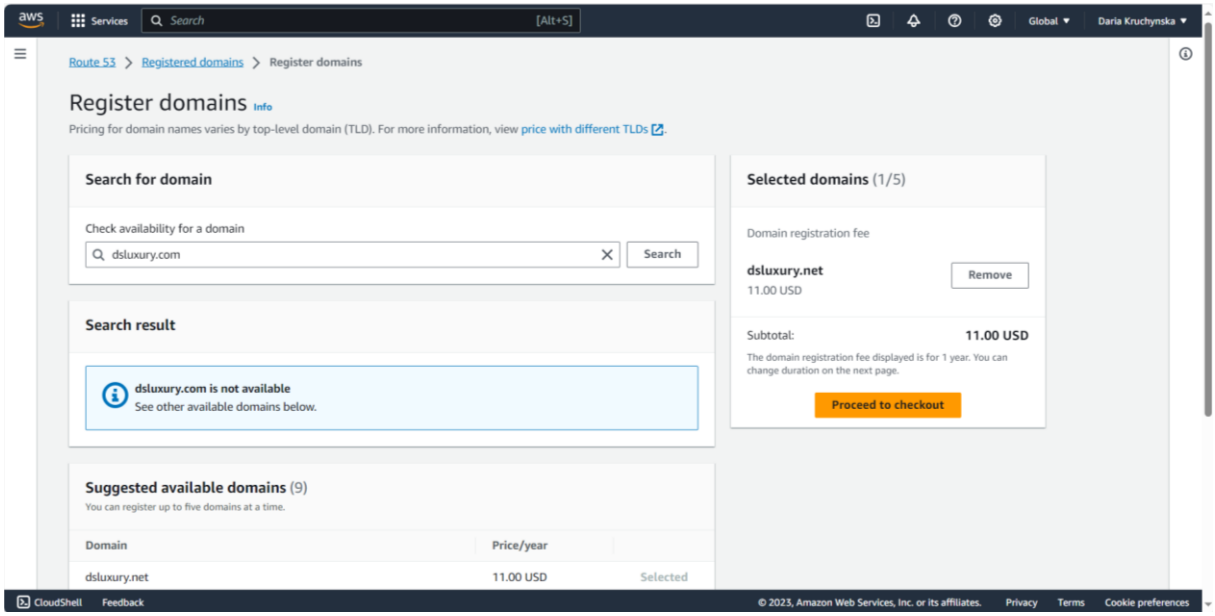

Рисунок 3.1.23 – Вибір доменного імені

Після того як доменне ім’я обрано, необхідно налаштувати оплату даного доменного імені. Цей процес включає в себе 3 кроки. На першому кроці відбуваються налаштування оплати, які показані на рисунку 3.1.24, а саме обрання терміну дії доменного імені, в нашому випадку це один рік.

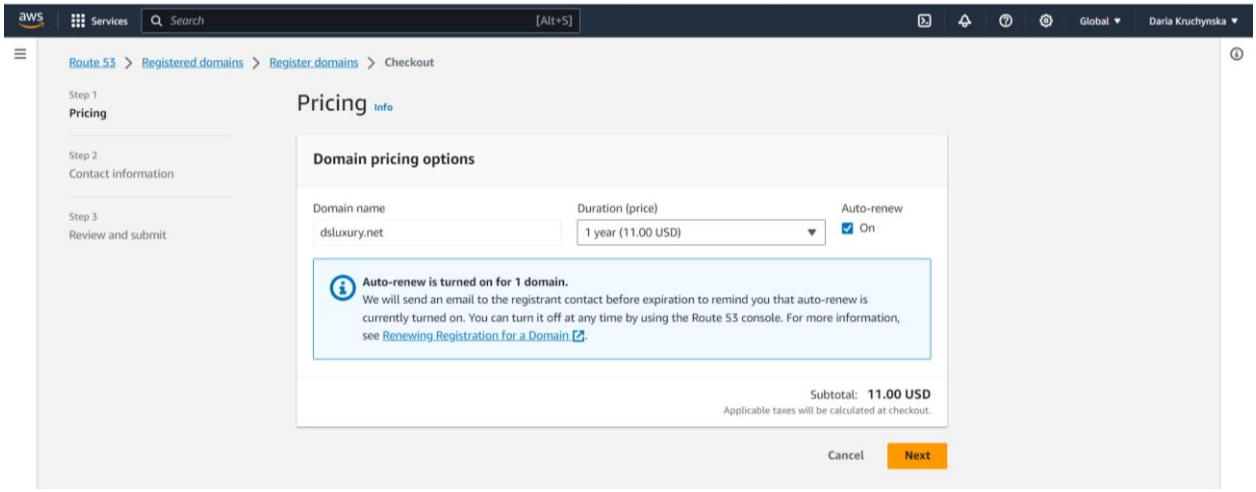

Рисунок 3.1.24 – Налаштування оплати доменного імені

На другому кроці заповнюється персональна інформація, як на рисунку 3.1.25, а саме прізвище та ім’я, електронна адреса, номер телефону та дані кредитної карти для оплати. В цілях безпеки деяка інформація замальована, а інша не показана.

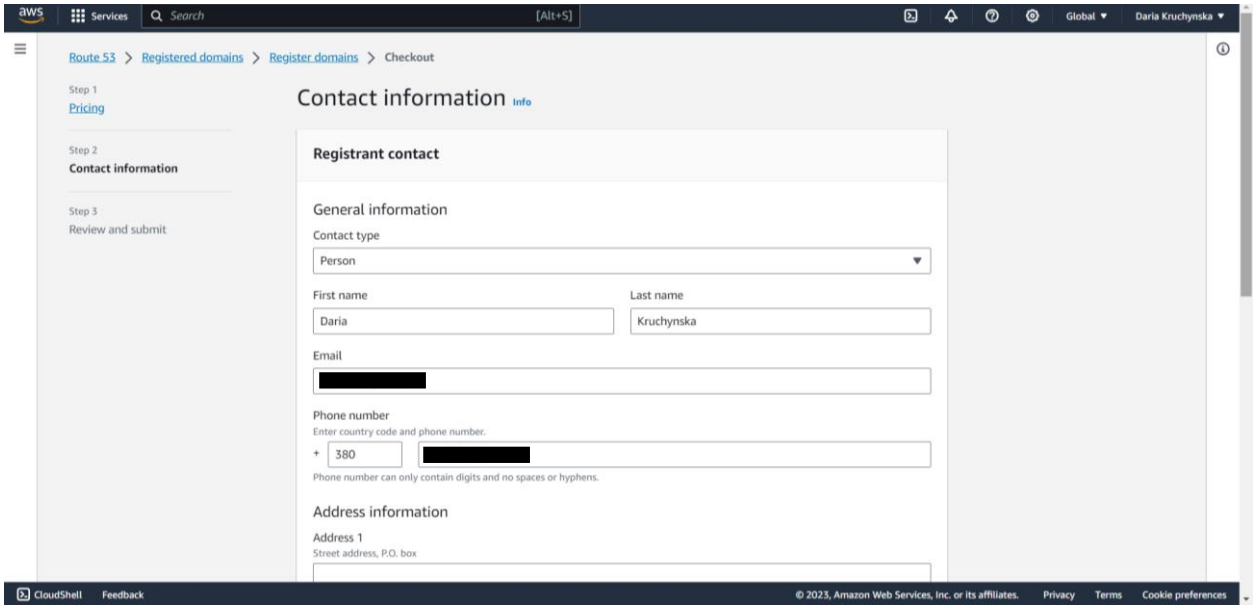

Рисунок 3.1.25 – Заповнення персональної інформації

І на останньому кроці, тобто третьому, який показаний на рисунку 3.1.26, відбувається перевірка усіх даних та підтвердження для створення доменного імені та зняття плати за нього з кредитної карти.

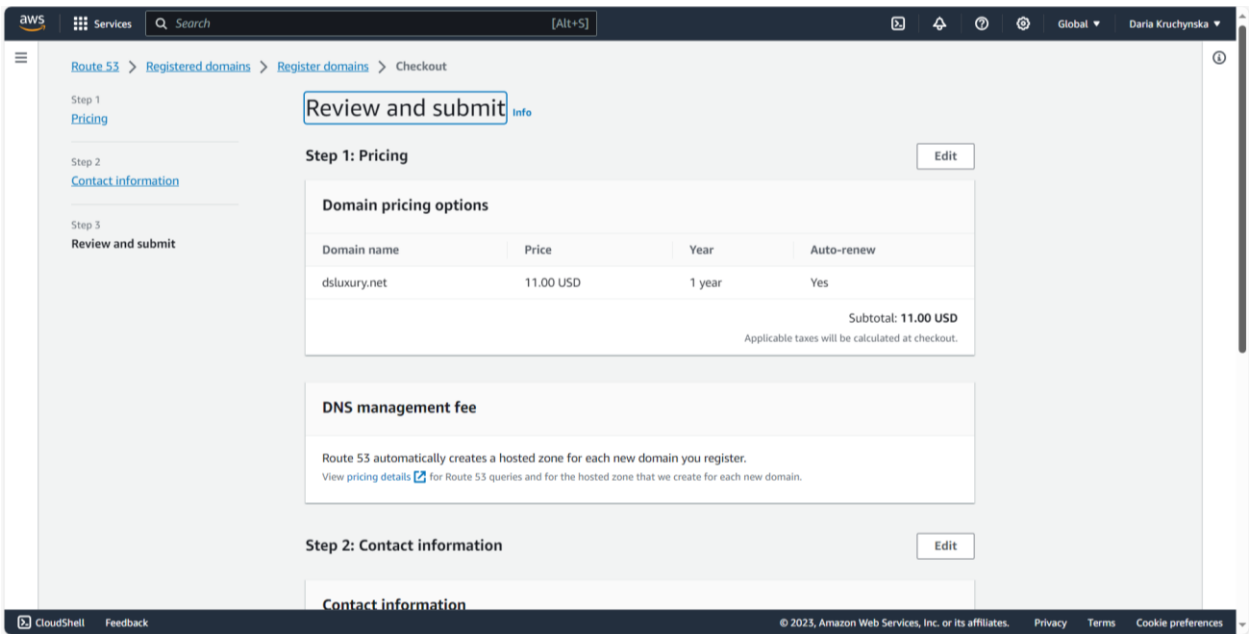

Рисунок 3.1.26 – Перевірка усіх кроків та підтвердження створення доменного імені

Після усіх кроків та підтвердження оплати з кредитної карти як на рисунку 3.1.27, ми отримуємо повідомлення, що створене доменне ім’я у процесі реєстрації, як на рисунку 3.1.28, це займає деякий час.

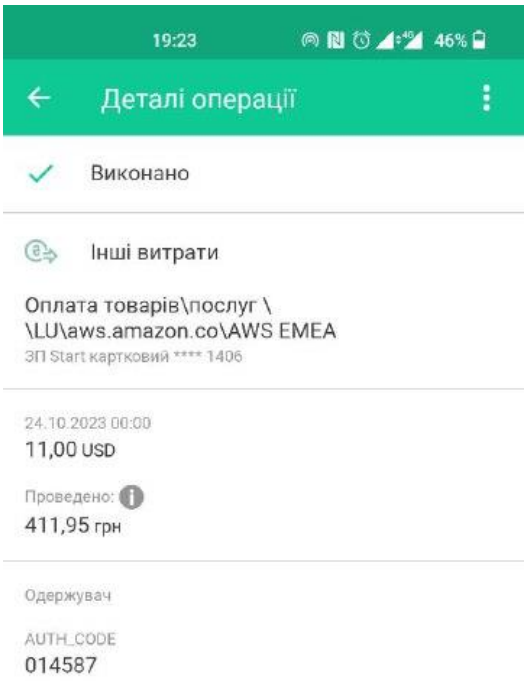

Рисунок 3.1.27 – Оплата доменного імені на рік

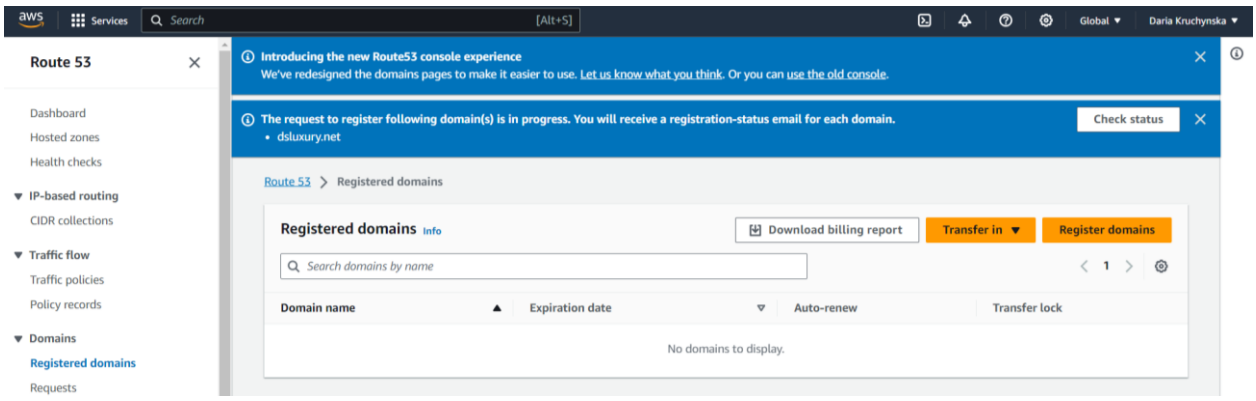

Рисунок 3.1.28 – Доменне ім’я у процесі реєстрації

3.2 Розгортання клієнтської інфраструктури

В основі більшості додатків використовується клієнт-серверна архітектура, яка складається з клієнтської та серверної частин, які використовують мережеве з’єднання, яке допомагає реалізовувати взаємодію та обмін інформацією між даними компонентами.

Клієнт може являти собою, наприклад, комп’ютер який буде на стороні саме користувача, за допомогою якого здійснюється запит до сервера, для надання відповідної інформації, або ж реалізації певних дій.

У системі, яка використовує таку модель, клієнт не тільки відправляє запит на сервер, де в подальшому він обробляється, а ще й отримує готовий результат від сервера. Клієнтська частина у свою чергу має ряд функцій, які реалізовуються, наприклад:

- надання інтерфейсу користувача;
- реалізація запиту до сервера та його відправка;
- отримання відповіді від сервера та відправка додаткових команд;
- тощо.

Розгортання клієнтської інфраструктури, представляє собою електронну комерцію на веб-рівні. Іншими словами реалізовується адаптивний веб-інтерфейс, який створений на основі технологій інтерфейсу таких як, наприклад, NodeJS, ReactJS тощо, та розгортається на основі такого сервісу як ***AWS Fargate***.

Сервіс AWS Fargate – це ядро для безсервісних обчислень, яке відбувається на базі контейнерів. Даний сервіс співпрацює як з сервісами Amazon Elastic Container Service (ECS) та Amazon Elastic Kubernetes Service (EKS), що є зручним. Використання сервісу AWS Fargate надає можливість сконцентрувати свою увагу саме на створенні додатка, так як не потрібно виділяти сервіси та керувати ними.

Amazon Elastic Container Service (ECS) — це масштабований та швидкий сервіс керування контейнерами, який спрощує запуск, зупинення та управління контейнерами у кластері.

Для початку використання сервісу AWS Fargate у сервісі Amazon Elastic Container Service (ECS) необхідно створити кластер для подальшої роботи, аби мати можливість запуску у ньому відповідних компонентів. Для цього необхідно нажати відповідну кнопку “Create cluster”, як на рисунку 3.2.1.

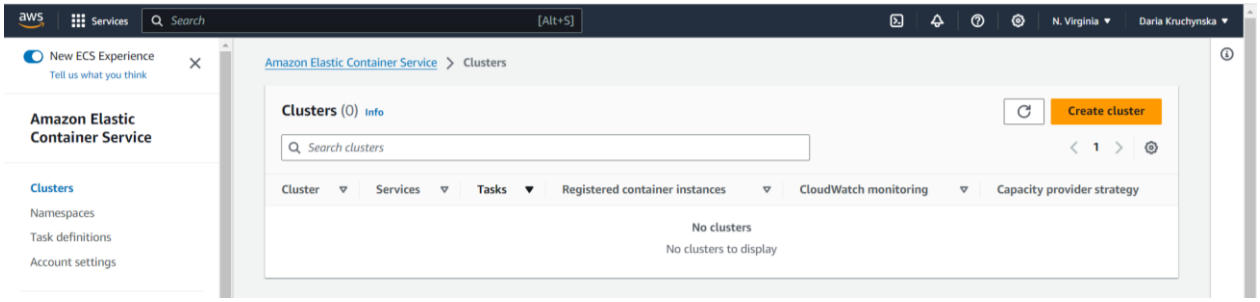

Рисунок 3.2.1 – Створення кластера для клієнтської частини

Після того як відкриється вкладка налаштування кластера, яке відображається на рисунку 3.2.2, необхідно дати йому назву, в нашому випадку дамо назву “dsluxury-1” та оберемо AWS Fargate, тобто без сервера. Це є зручним, адже плата буде зніматись за ті навантаження, які використовуються у контейнері, а не за цілий сервер.

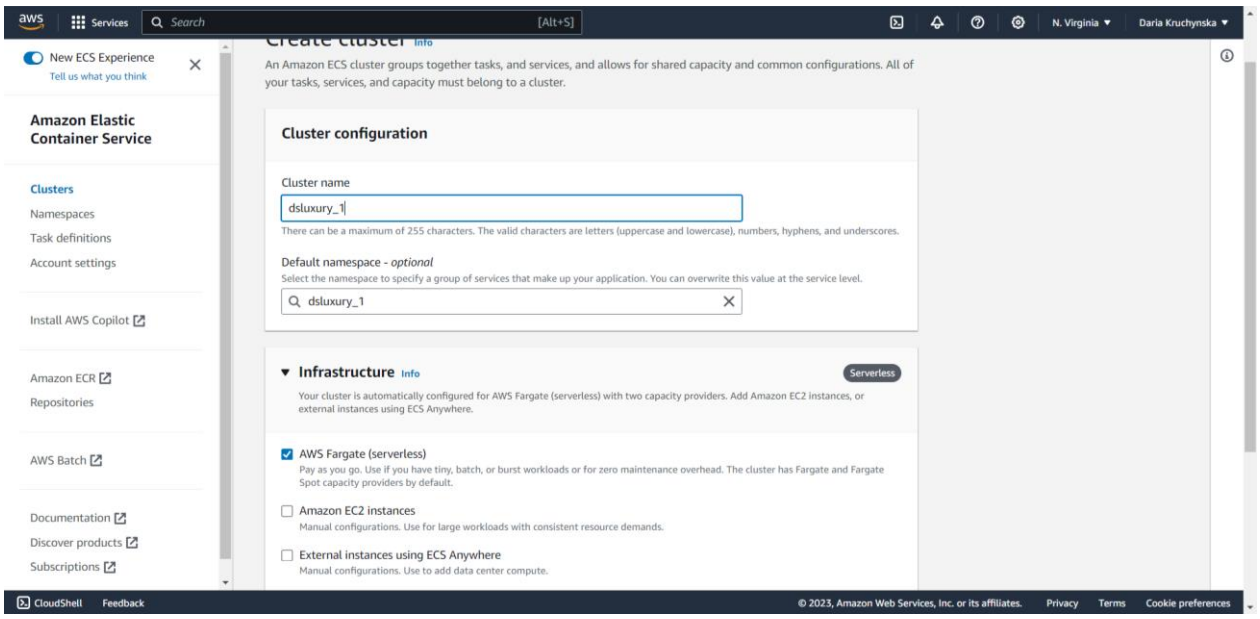

Рисунок 3.2.2 – Налаштування кластера для клієнтської частини

Після налаштувань необхідно створити кластер, натиснувши відповідну кнопку внизу та якщо все вірно, в результаті буде створено кластер, як на рисунку 3.2.3.

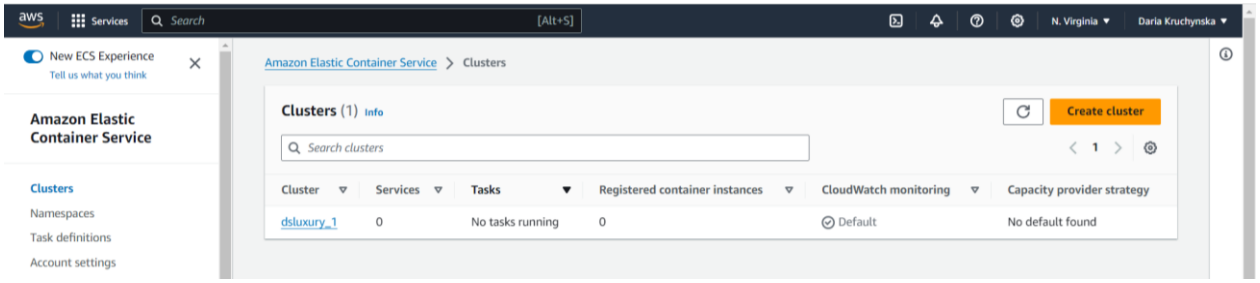

Рисунок 3.2.3 – Успішно створений кластер для клієнтської частини

Після того як кластер створено, можна перейти до створення саме того, що ми будем запускати у кластері, а саме клієнтську частину. Відповідно для початку необхідно перейти до створення, для чого потрібно нажати кнопку “Create new task definition”, як на рисунку 3.2.4.

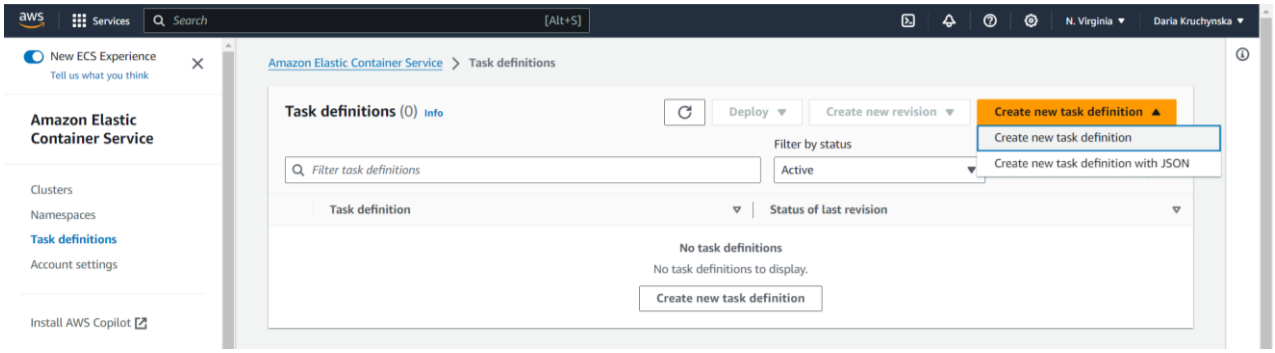

Рисунок 3.2.4 – Створення завдання для клієнтської частини

Далі необхідно виконати налаштування завдання, які на рисунку 3.2.5, для початку надати логічну назву, в нашому випадку “dsluxury-frontend” та обрати відповідну інфраструктуру для контейнерів.

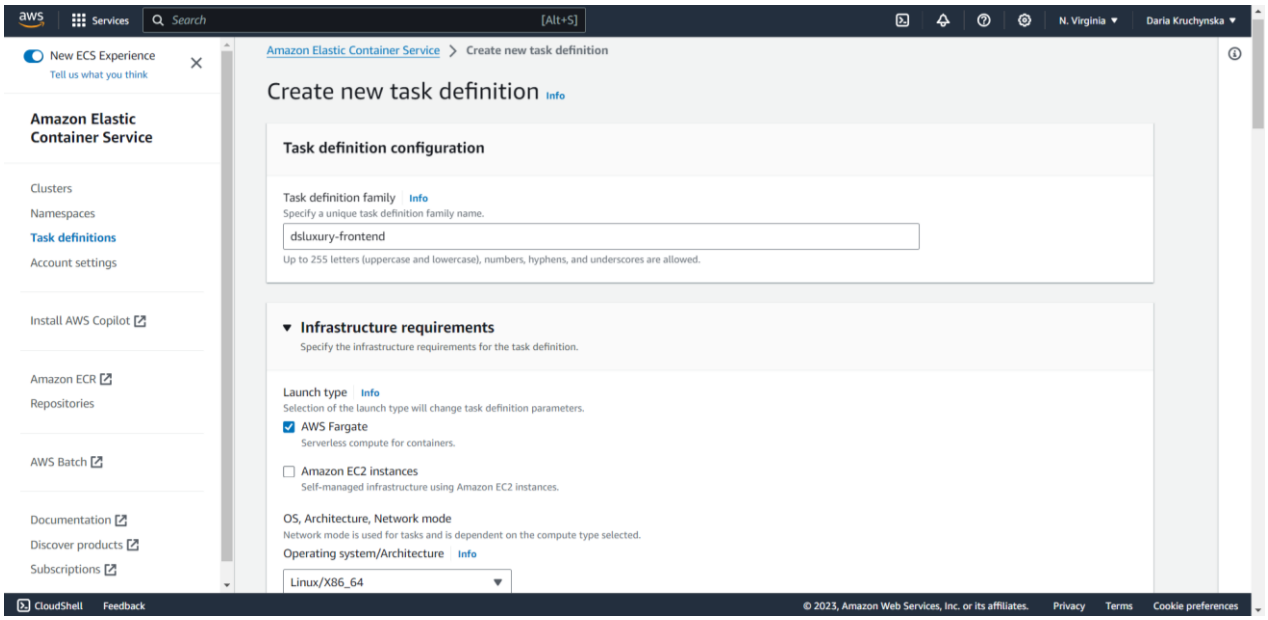

Рисунок 3.2.5 – Налаштування завдання для клієнтської частини

Далі налаштовуються розміри завдання на рисунку 3.2.6, в якому обираються об’єм CPU та GB, який буде використовуватись кожну годину, та за яку в кінці місяця будуть вираховуватись кошти. В нашому випадку це найменші значення, адже це є економічно вигідно та на даному етапі розробки достатньо для реалізації хмарної інфраструктури.

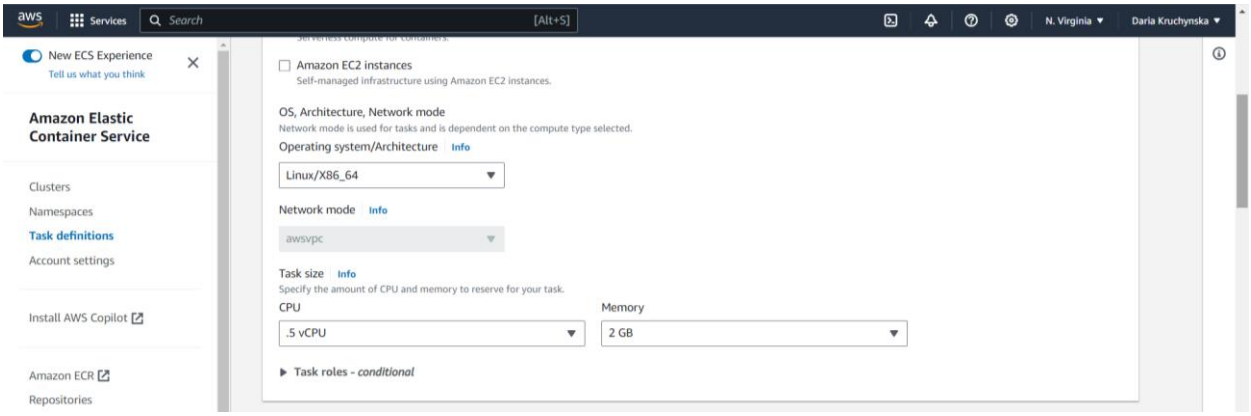

Рисунок 3.2.6 – Налаштування розмірів для клієнтської частини

Після налаштувань розміру завдання, необхідно додати сам контейнер який надалі буде запускатись у раніше створеному кластері. Додавання контейнера та налаштування порту запуску реалізовано на рисунку 3.2.7.

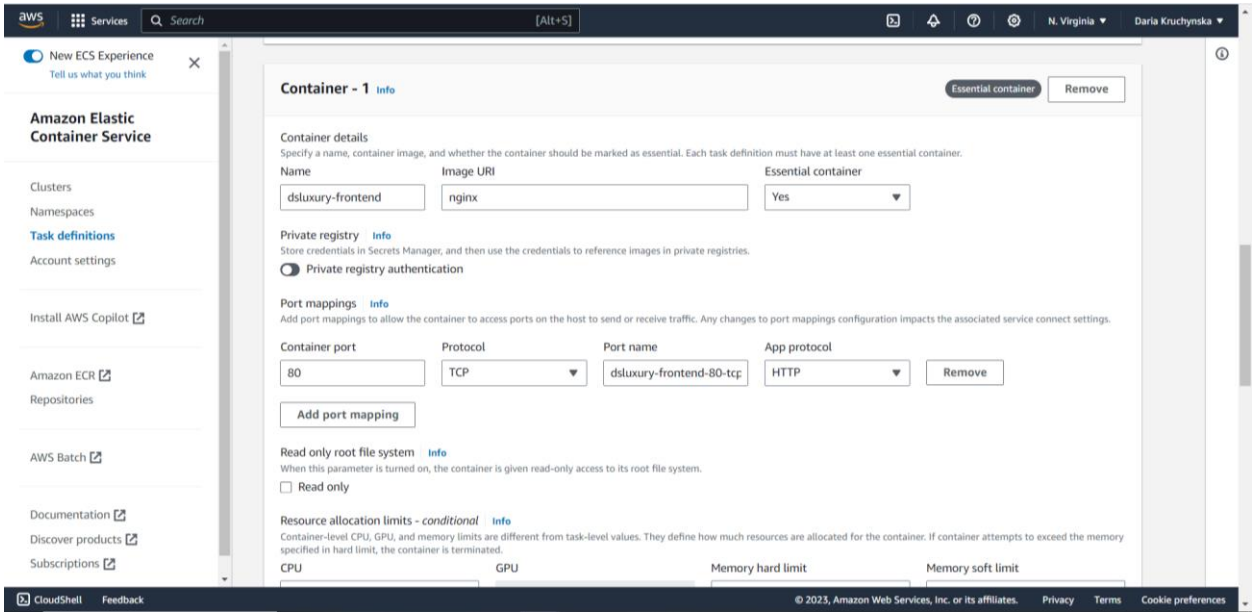

Рисунок 3.2.7 – Додавання контейнера для клієнтської частини

Після того як всі налаштування завершені та відсутні помилки відбувається успішне створення завдання, як на рисунку 3.2.8.

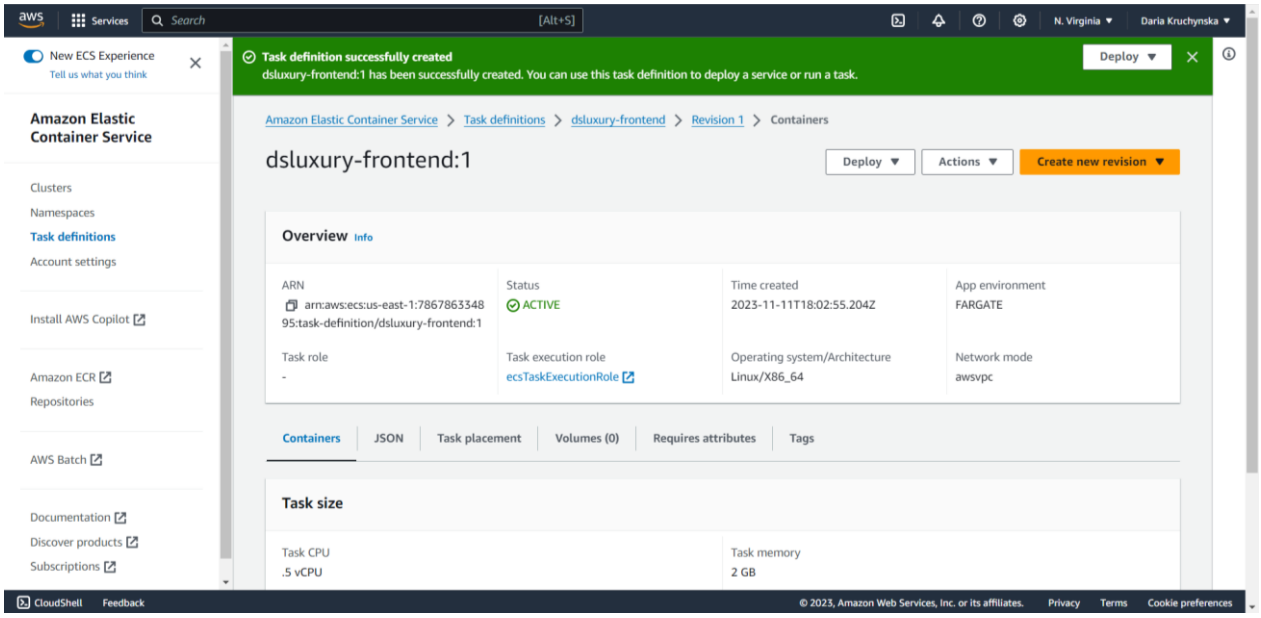

Рисунок 3.2.8 – Успішно створене завдання для клієнтської частини

Оскільки вже створено кластер та завдання, тепер у створеному кластері необхідно запустити наше створене завдання, яке на рисунку 3.2.8. Для цього необхідно перейти у створений кластер та відповідно на вкладці завдань, натиснути кнопку для запуску завдання, як на рисунку 3.2.9.

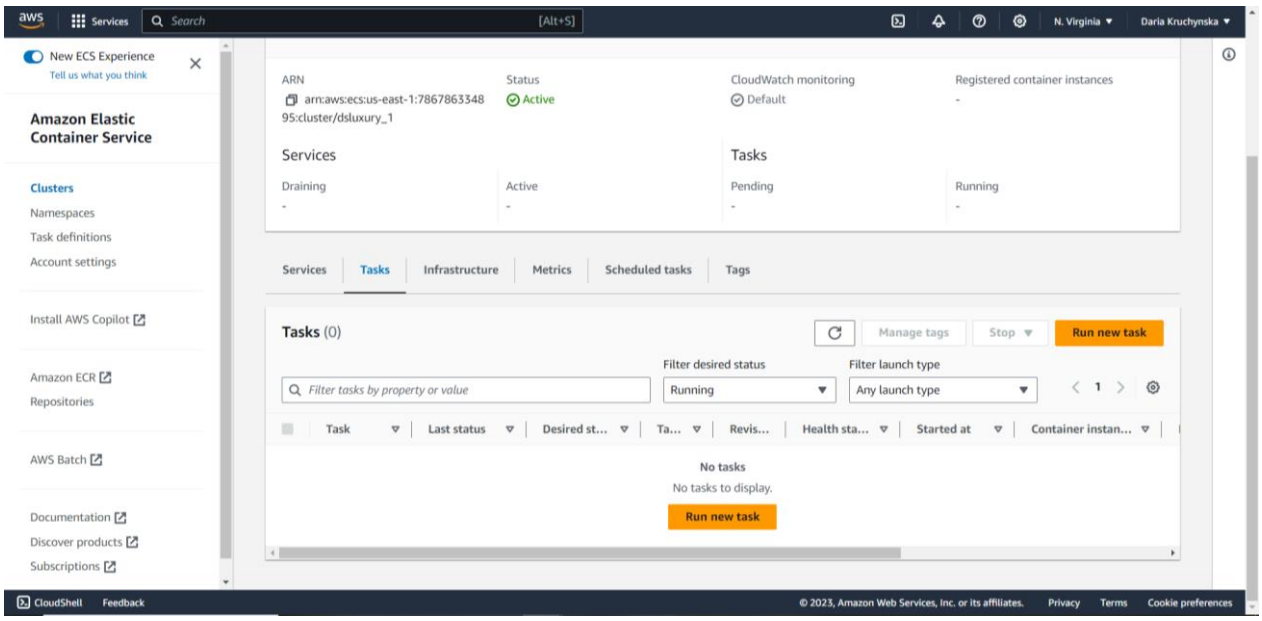

Рисунок 3.2.9 – Запуск завдання для клієнтської частини

Тепер необхідно виконати налаштування для запуску завдання, для початку необхідно обрати параметр обчислень, як на рисунку 3.2.10, в нашому випадку це варіант запуску завдання без використання стратегії постачальника потужностей, адже це економічно вигідно на даному етапі розробки.

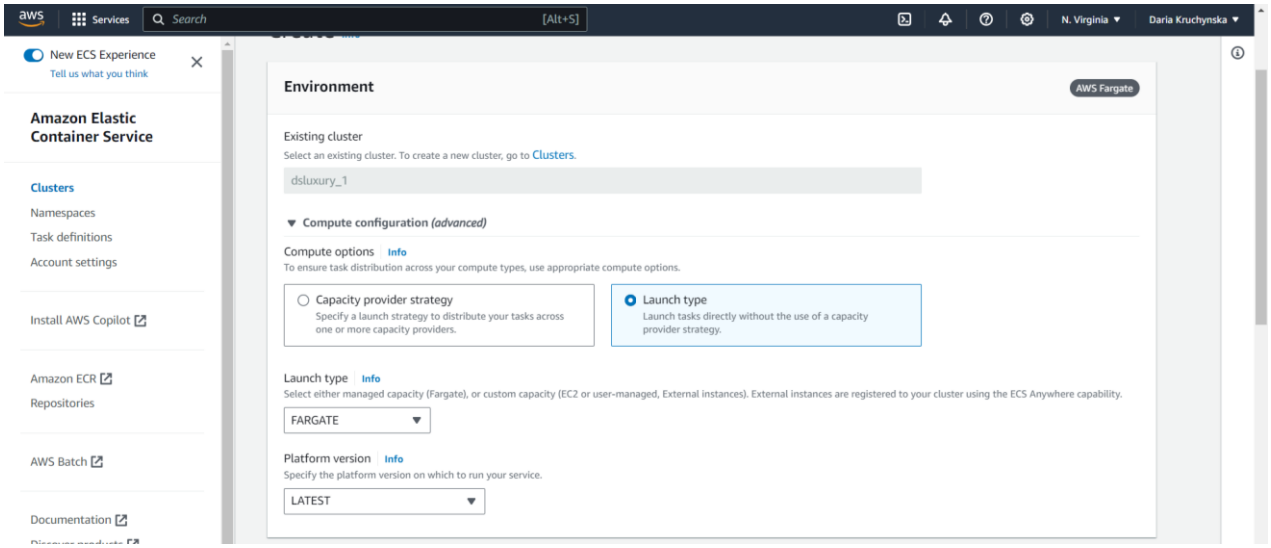

Рисунок 3.2.10 – Обрання параметрів обчислення для клієнтської частини

Наступним налаштовується конфігурація розгортання на рисунку 3.2.11. Відповідно розгортається завдання, яке було створено на рисунку 3.2.8, яке буде одне на даному етапі розробки.

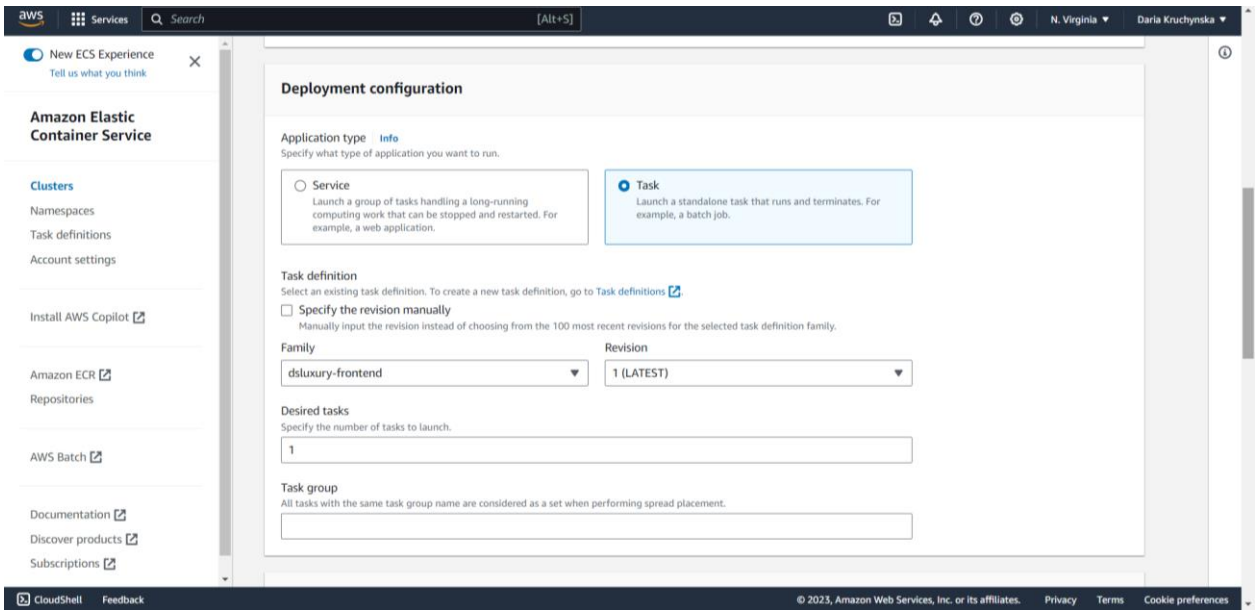

Рисунок 3.2.11 – Налаштування конфігурації розгортання для клієнтської частини

Після цього необхідно налаштувати параметри мережі, де саме буде запускатись завдання, відповідно на рисунку 3.2.12 показані налаштування мережі.

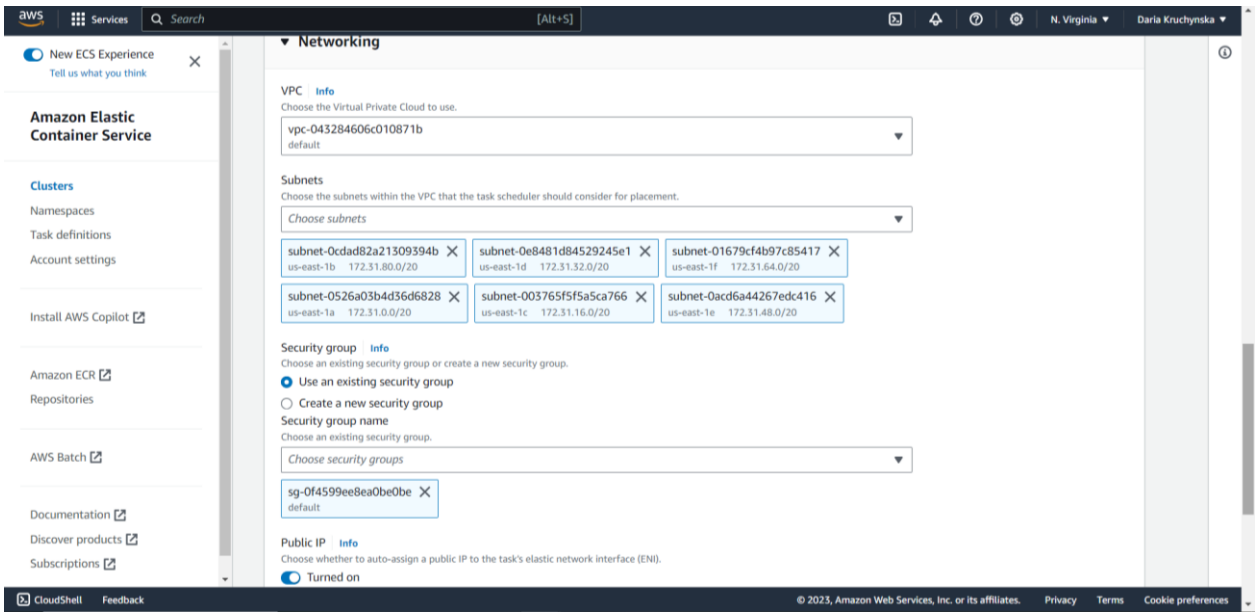

Рисунок 3.2.12 – Налаштування мережі для клієнтської частини

Налаштування завершені, тому після натискання відповідної кнопки отримано результат на рисунку 3.2.13, що наше завдання яке було створено раніше на рисунку 3.2.8, успішно запустилось у кластері, який ми створили на рис. 3.2.3.

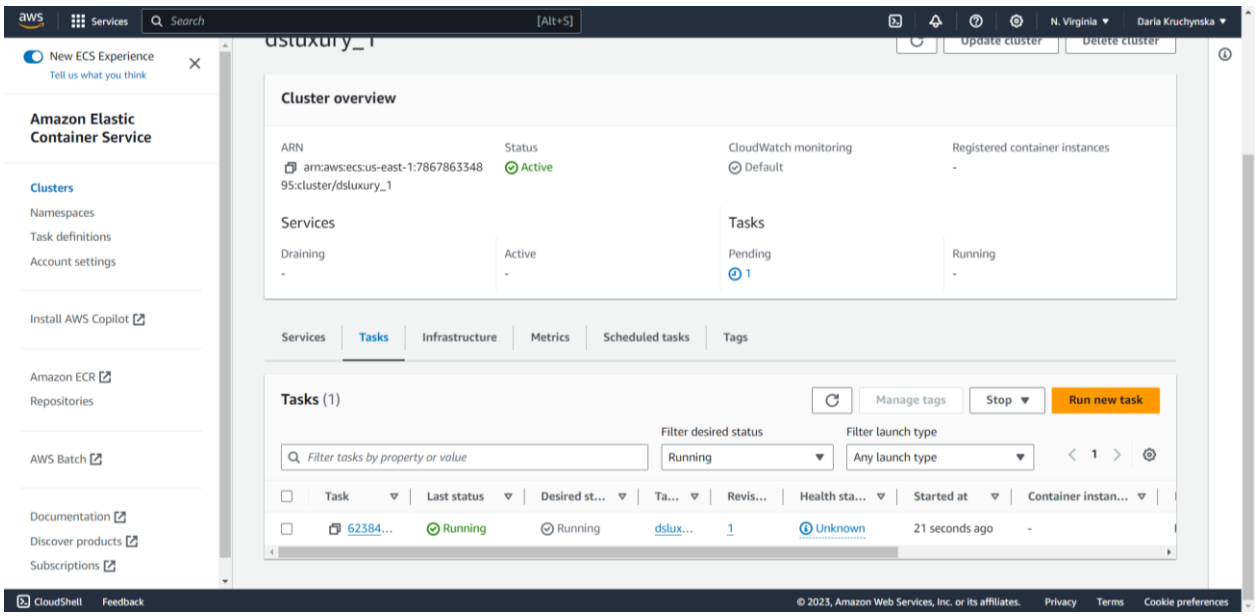

Рисунок 3.2.13 Успішно запущене завдання у кластері для клієнтської частини

В клієнтській частині використовується також сервіс ***Amazon ElastiCache,*** саме для кешування статичного вмісту та організованих відповідей API серверної частини. Amazon ElastiCache є сервісом який спрощує налаштування, керування та масштабування сховищ даних у пам'яті, або ж області кешування в хмарі. Даний сервіс використовується для кешування, але в той самий час він допомагає ліквідувати складнощі, які пов'язані з розгортанням та керуванням областю розподіленого кешу.

Для початку роботи з даним сервісом необхідно обрати сховища даних, як на рисунку 3.2.14, в нашому випадку це Redis, так як він має більше переваг та можливостей ніж Memcashed, тому цей вибір є доцільним.

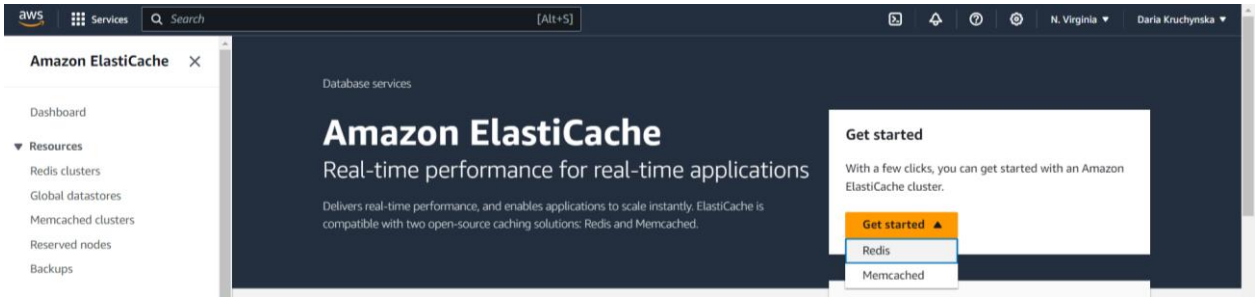

Рисунок 3.2.14 – Налаштування кешування даних для клієнтської частини

На початку налаштування сервісу, необхідно обрати конфігурацію та метод створення кластера, як на рисунку 3.2.15. На даному етапі розробки

доцільно обрати демо конфігурацію, так як цього буде достатньо, та легкий спосіб створення кластера.

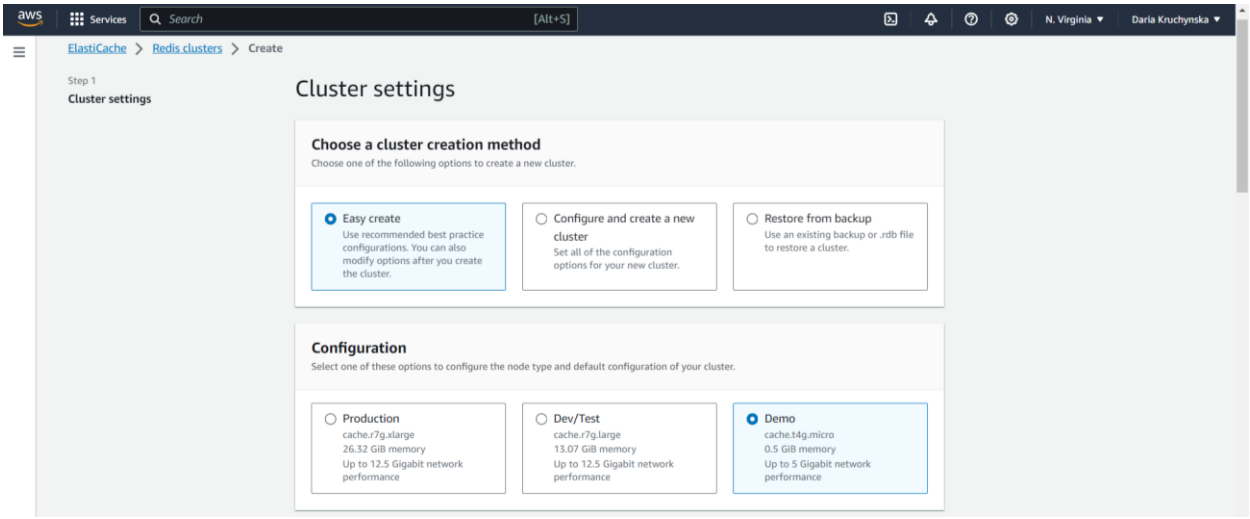

Рисунок 3.2.15 – Обрання методу створення кластера та конфігурації для клієнтської частини

Далі необхідно ввести певні дані для налаштування кластера, як на рисунку 3.2.16, зокрема назву та опис кластера.

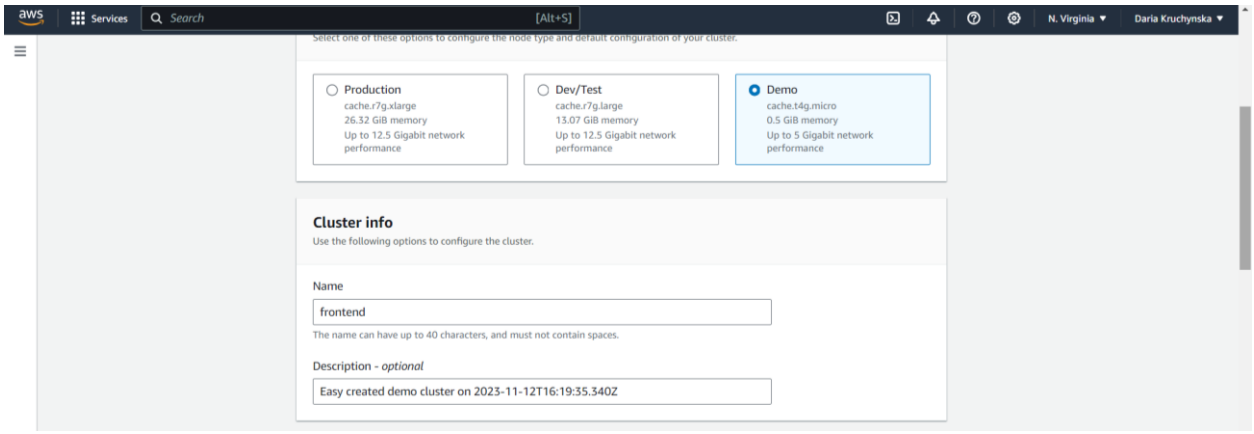

Рисунок 3.2.16 – Налаштування інформації про кластер для клієнтської частини

Після того як основні дані введенні, потрібно обрати відповідні параметри для мережевого зв’язку з кластером, як на рисунку 3.2.17. В даному випадку підключення можливо за протоколом IPv4. Далі створено набір підмереж для кластерів, які будуть працювати у віртуальних приватних хмарах.

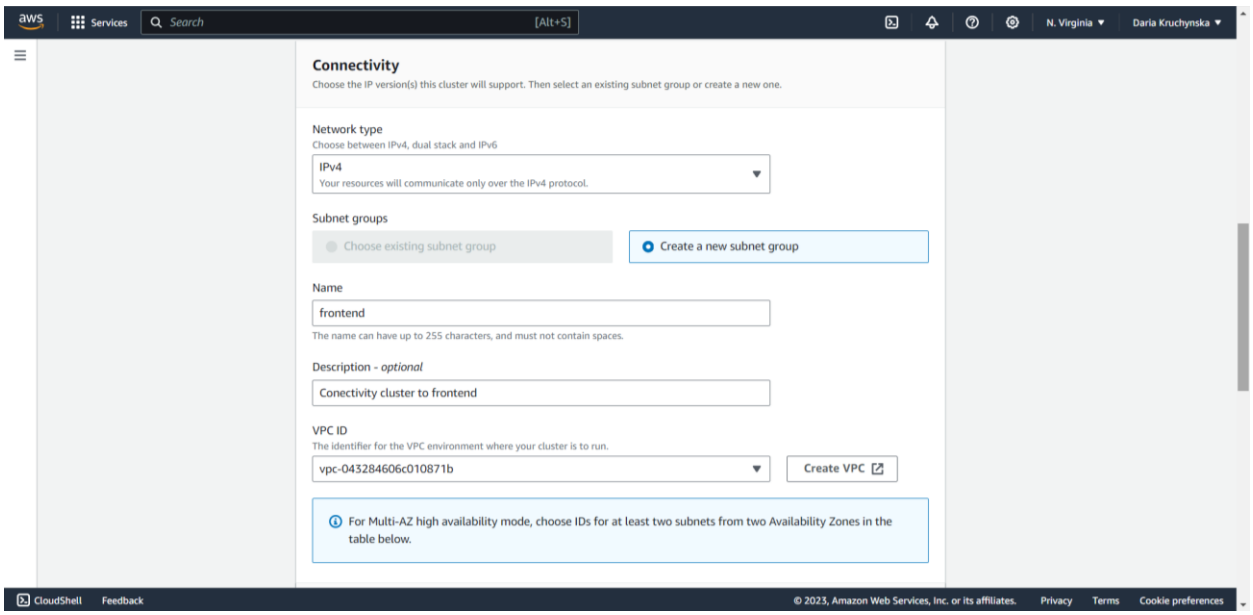

Рисунок 3.2.17 – Налаштування мережевого зв’язку з кластером для клієнтської частини

Після того як мережевий зв’язок налаштовано, необхідно обрати відповідні підмережі, та налаштувати їх для відповідних зон доступності, як на рисунку 3.2.18.

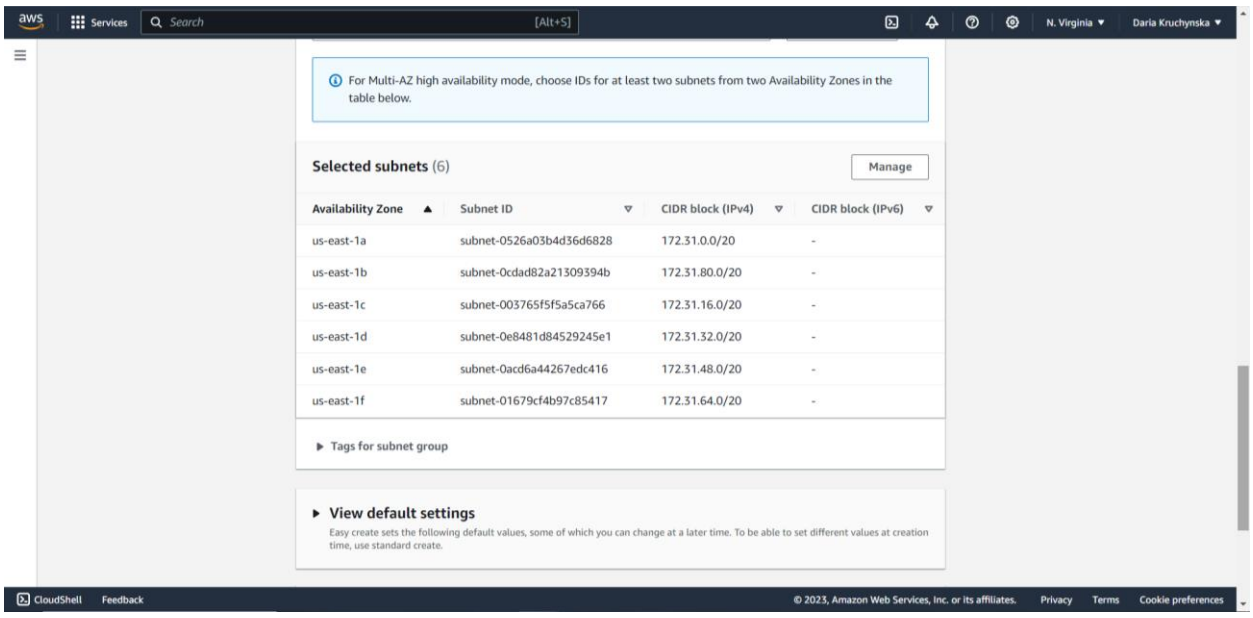

Рисунок 3.2.18 – Налаштування підмереж у зонах доступності для клієнтської частини

Після того як всі налаштування завершено, отримується успішно створений кластер для кешування даних, як на рисунку 3.2.19.

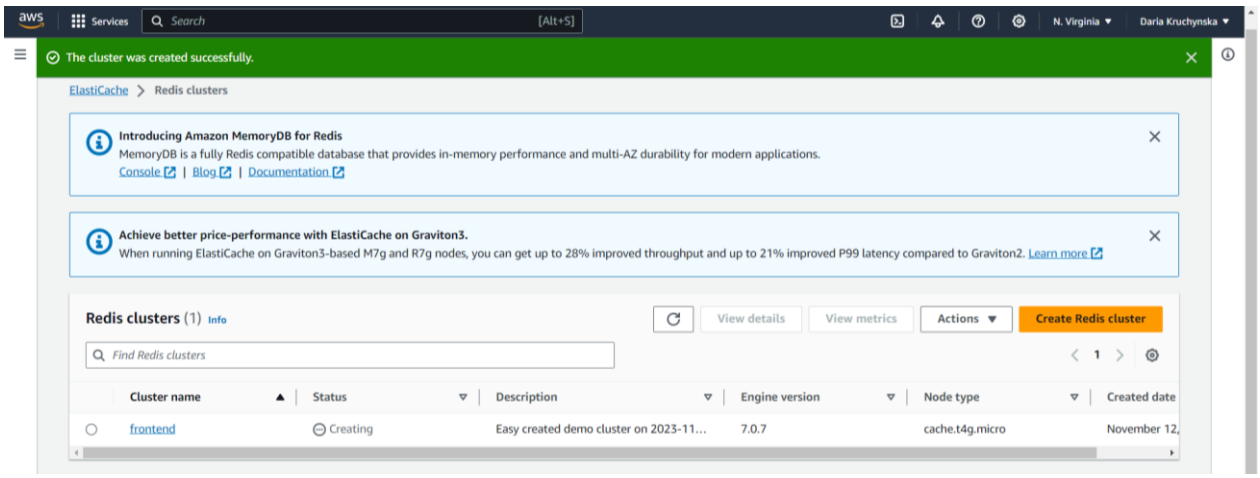

Рисунок 3.2.19 – Успішно створений кластер для кешування даних у клієнтській частині

Майже усі додатки, мають базу даних і звичайно хмарна інфраструктура даного додатку не є винятком. Для реалізації хмарної БД є сервіс ***Amazon DynamoDB***. Даний сервіс використовується додатками, які потребують найменшу затримку даних у будь-якому масштабі. Amazon DynamoDB є швидким та гнучким сервісом БД NoSQL для різноманітних додатків.

Розгортання сервісу Amazon DynamoDB у клієнтській частині реалізовується для збереження сеансів користувачів, або ж іншими словами сесії користувачів та самих конфігурацій зовнішньої частини додатка, наприклад, це можуть бути позначки функції, або ж іншими словами флажки. Але на даному етапі розробки проєкту реалізовується лише частина БД з сесіями користувачів, так як позначки функції доцільно реалізовувати вже під потреби конкретного інтернет-магазину.

У клієнтській частині сервіс Amazon DynamoDB буде використовуватись у якості сховища сесії користувачів, що дозволить зберігати інформацію під час сеансів перегляду веб-сторінок додатка у майбутньому. Перевагою даного сервісу є швидке та масштабоване керування розподіленими сеансами користувачів. Також важливо, що даний сервіс реалізовується як платформа єдиного входу, замість підтримки окремих локальних магазинів, що в свою чергу позитивно впливає на низку факторів, як витрати, зручність і т.д. Доступ до сховища сеансів, буде містити наступну інформацію:

- створення запису для сеансу користувача;
- пошук сеансів користувачів;
- список всіх дочірніх сеансів для сеансів користувачів;
- отримання часу останнього входу в систему для користувачів.

Для створення таблиць у сервісі Amazon DynamoDB, необхідно нажати відповідну кнопку як на рисунку 3.2.20, для переходу до процесу створення.

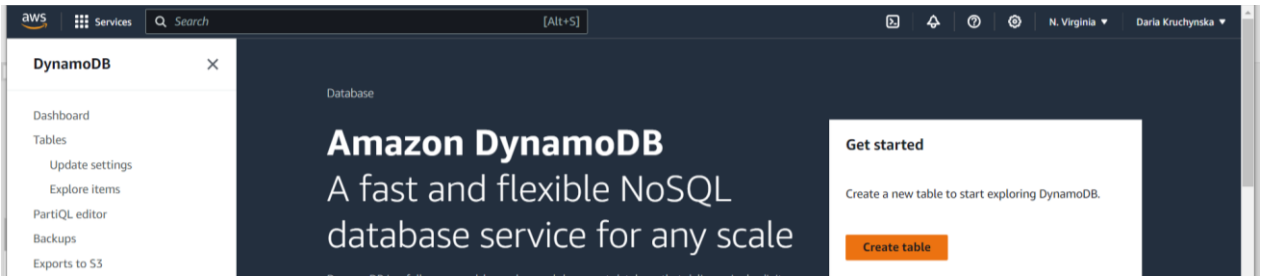

Рисунок 3.2.20 – Початок створення таблиць

Першою таблицею створюється таблиця користувачів. На рисунку 3.2.21 задається назва таблиці та додаткова інформація, така як ключове поле та сортувальні, й відповідно їх типи даних.

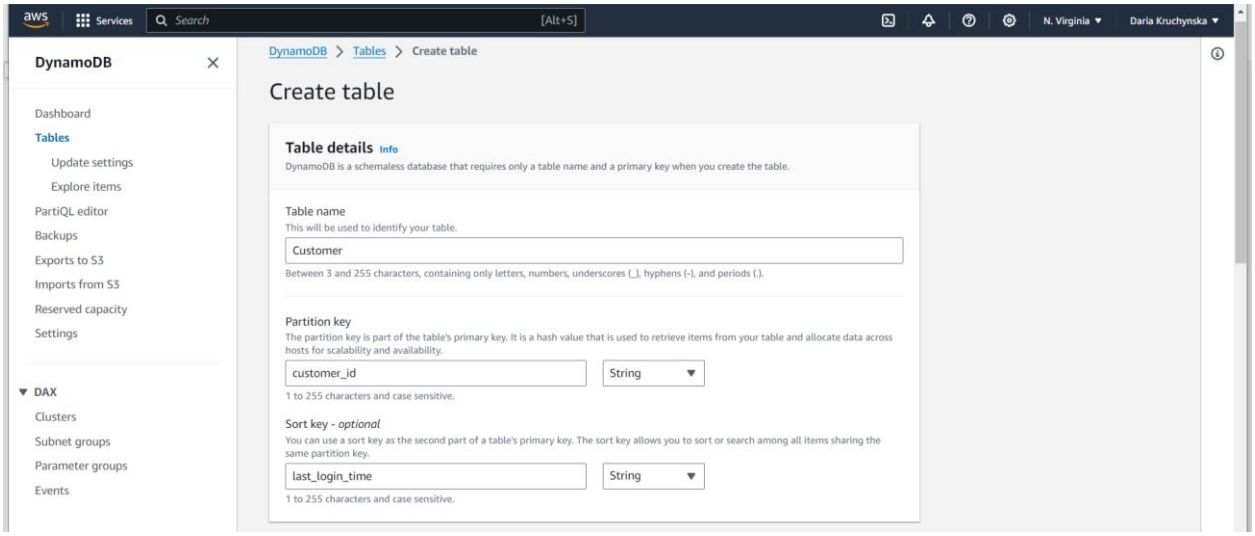

Рисунок 3.2.21 – Створення таблиці “Customer”

Далі для створення таблиці її налаштування залишаються за замовчуванням, як на рисунку 3.2.22, дані налаштування будуть і для всіх наступних таблиць, так як це є доцільним на початковому етапі розробки, та в майбутньому може бути зміненим, та відредагованим під потреби конкретного інтернет-магазину.

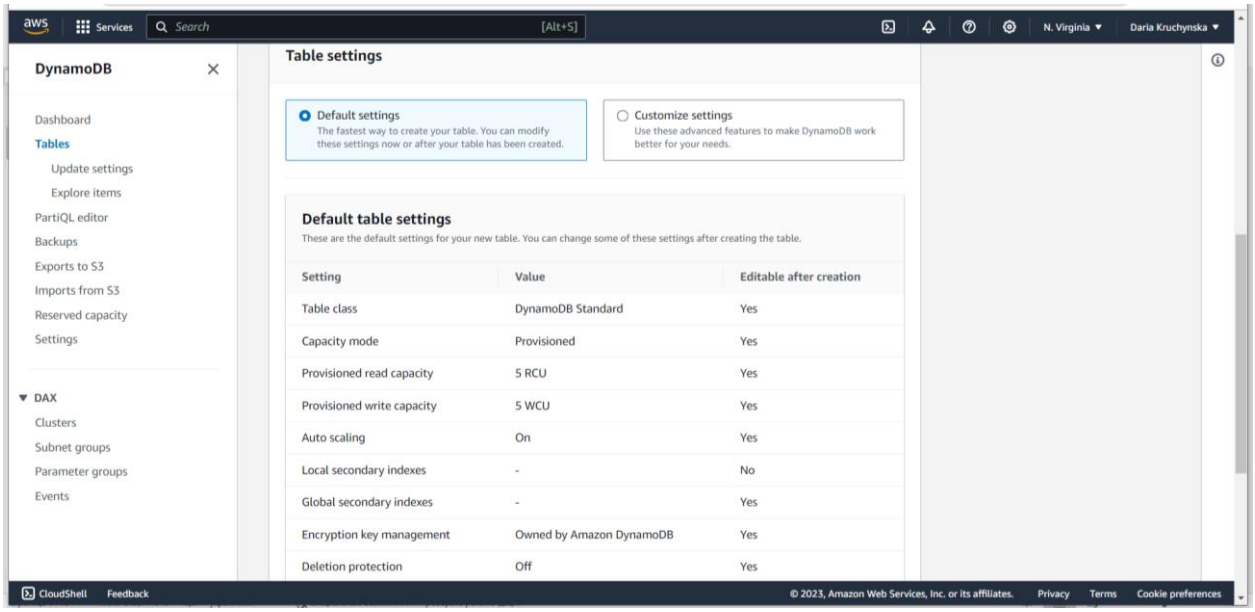

Рисунок 3.2.22 – Налаштування таблиць за замовчуванням

Після реалізації усіх налаштувань створюється відповідна таблиця, як на рисунку 3.2.23.

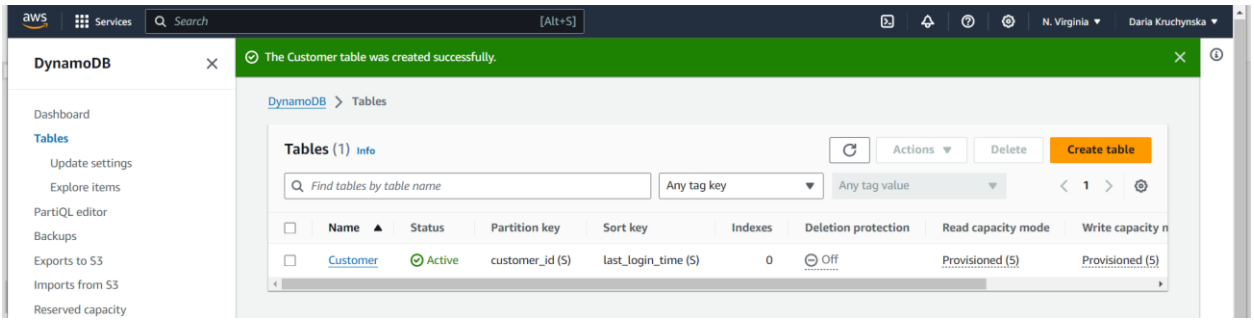

Рисунок 3.2.23 – Успішно створена таблиця “Customer”

Наступними необхідно створити таблицю сесій та дочірніх сесій, процес початку створення відбувається як на рисунку 3.2.20, а далі налаштування повторюються як на рисунку 3.2.21 та рисунку 3.2.22, але з відповідними назвати і т.д. Після чого отримуємо успішно створені таблиці сесій та дочірніх сесій на рисунку 3.2.24, для майбутнього збереження сесій користувачів.

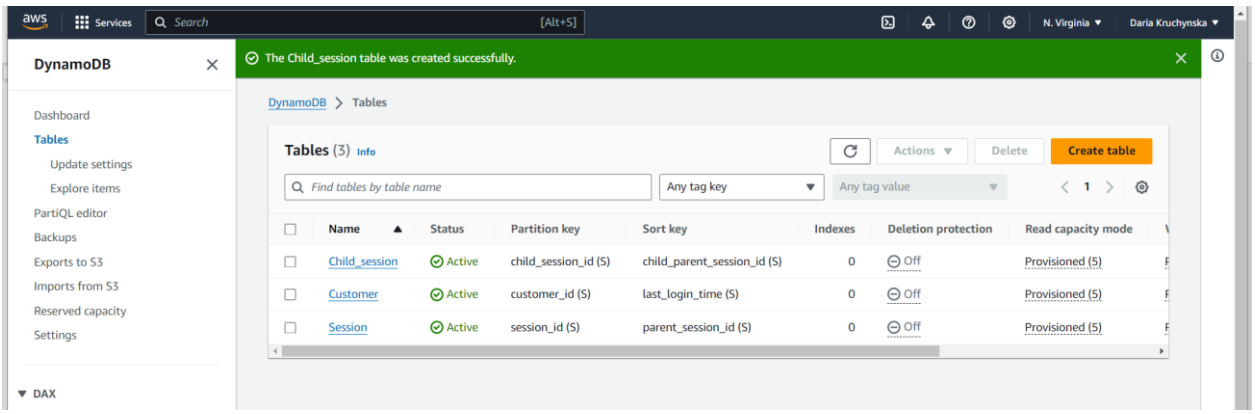

Рисунок 3.2.24 – Успішно створена таблиця “Session” та “Child_session”

3.3 Розгортання серверної частини

Як зазначалось вже у розділі 3.2, що більшість застосунків обирають в основі клієнт-серверну архітектуру. Окрім клієнта в даній архітектурі звичайно має місце і сервер.

Сервером в такій архітектурі може бути спеціальне обладнання, або ж більш потужний комп’ютер, а може бути і якийсь інший прилад, який буду призначений саме для вирішення певних завдань чи задач. Перелік завдань які буде вирішувати сервер, звичайно залежить від потреб додатка, наприклад, це може бути надання користувачам доступу до певних ресурсів, або ж зберігання певних даних та БД, далі цей список може ще продовжуватись.

Сервер може одночасно отримувати декілька запитів, тому він може обслуговувати не тільки одного клієнта, а й інших одночасно. В залежності від випадку та налаштувань, запити можуть мати рівень пріоритетності, та виконуватись раніше за інші, поза чергою. Це є зручним, особливо для інтернет-магазинів, адже запити оплати будуть завжди у пріоритеті.

В загальному можна описати, які саме функції повинен виконувати сервер у клієнт-серверній архітектурі, зокрема:

- обробляти запити від клієнтів;
- надавати відповідь клієнту;
- виконувати різноманітні дії із даними, такі як збереження, захист, доступ та інші;

- тощо.

Серверна частина хмарної інфраструктури буде являти собою розгортання набору сервісів Restful, тобто інтерфейс для безпечного обміну інформацією у мережі, які в свою чергу будуть без збереження стану, створені саме для доступу до інформації, а також для виконання бізнес-логіки.

Дані мікросервіси будуть розгортатись у безсерверних обчислювальних службах, тобто за допомогою сервісів ***Amazon Fargate*** та ***AWS Lambda***. Використовуючи дані сервіси, можна реалізувати, наприклад, оформлення замовлення у кошику, або ж обробку платежів тощо.

Сервіс Amazon Fargate вже більш детально розглядався у розділі 3.2, саме за допомогою даного сервісу виникає можливість реалізувати все на базі безсерверних обчислень у контейнерах. Використання сервісу AWS Lambda дає можливість запустити майже будь-який програмний код додатка, а найголовніше не використовуючи сервер та не обслуговуючи його. Даний сервіс також безсерверний та створений для керування подіями обчислювальних сервісів.

Для початку необхідно створити кластер у сервісі Amazon Fargate, у якому в подальшому будуть запускатись необхідні компоненти. Початок створення кластера відповідно аналогічний до рисунка 3.2.1. Далі необхідно налаштувати кластер та обрати потрібну інфраструктуру, як на рисунку 3.3.1.

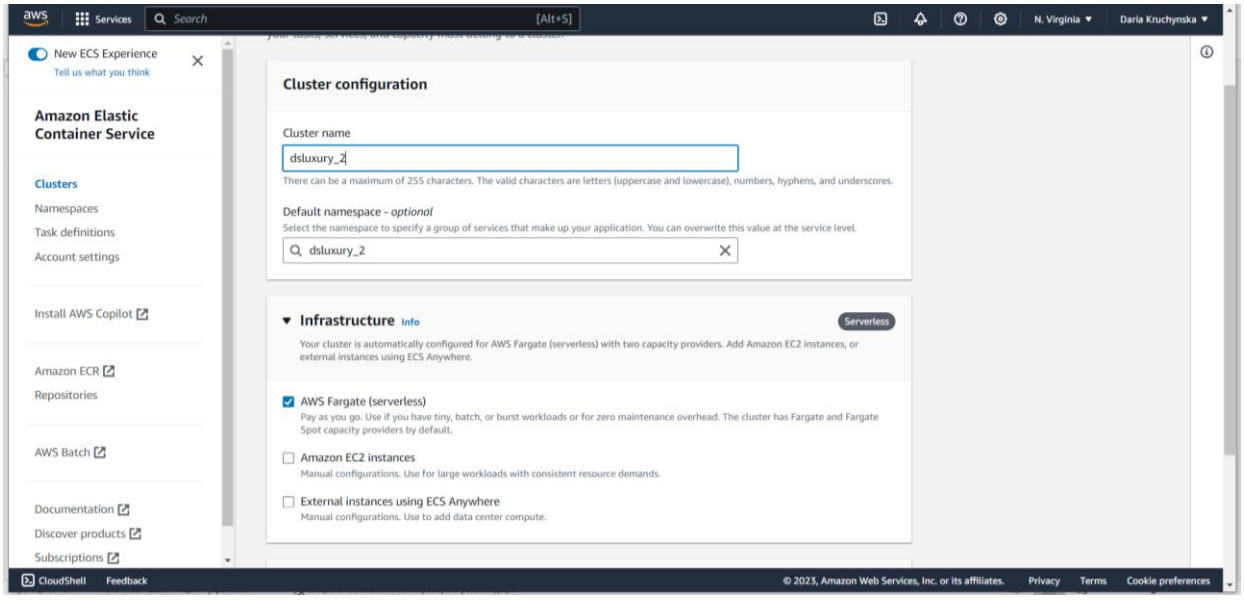

Рисунок 3.3.1 – Налаштування кластера для серверної частини

Після усіх налаштувань, кластер успішно створиться як на рисунку 3.3.2.

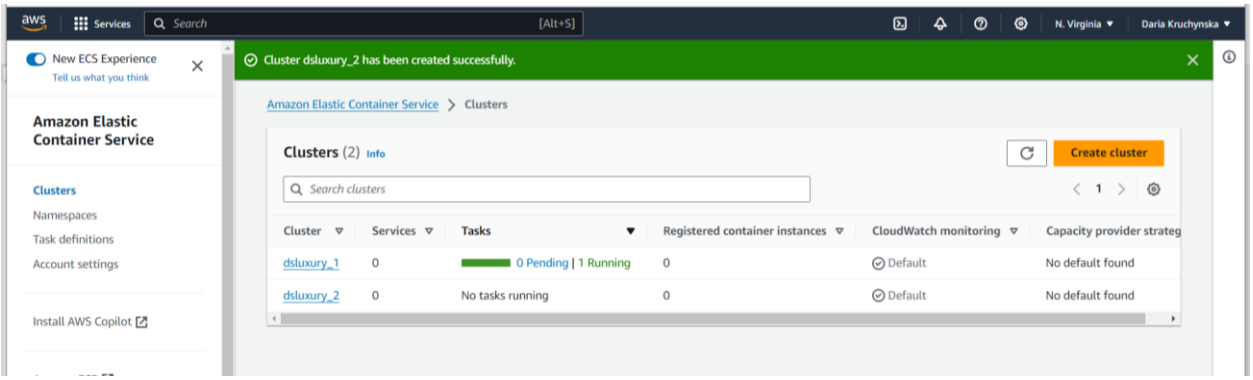

Рисунок 3.3.2 – Успішно створений кластер для серверної частини

Так як кластер для серверної частини вже створений, тепер можна перейти до створення завдань, які будуть запускатись саме у цьому кластері. Початок створення завдань аналогічний до рисунка 3.2.4. Після цього потрібно дати назву, яка буде відповідати серверній частині та обрати інфраструктуру для контейнера, як на рисунку 3.3.3.

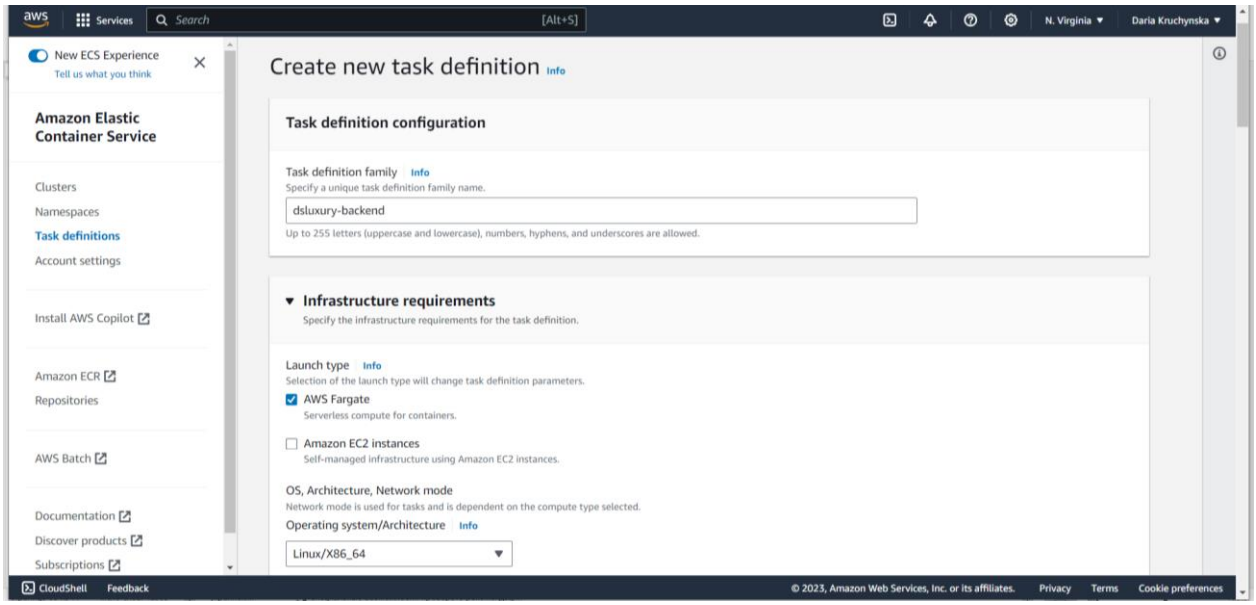

Рисунок 3.3.3 – Налаштування завдання для серверної частини

Далі налаштовуються розміри завдання, які будуть аналогічні як на рисунку 3.2.6, так як це є найбільш оптимально для даної розробки, і на цьому етапі. Після того як розмір налаштовано, потрібно додати контейнер, який буде запускатись у кластері серверної частини. Налаштування контейнера та порту запуску, показано на рисунку 3.3.4.

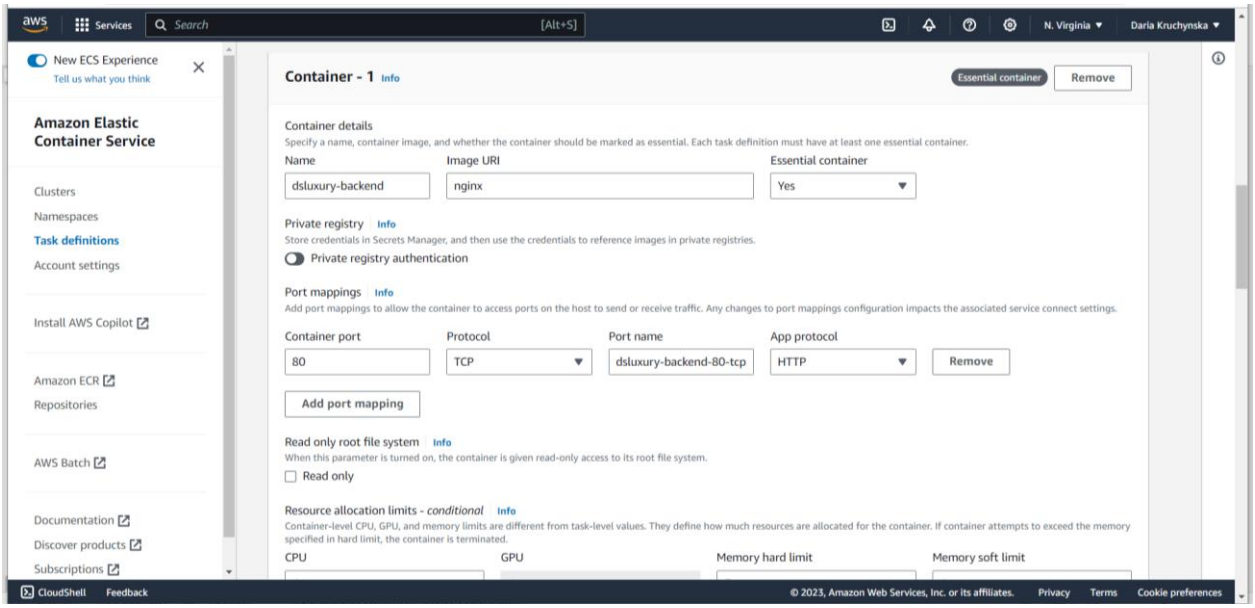

Рисунок 3.3.4 – Додавання контейнера для серверної частини

Так як всі налаштування завершені, то можна створити саме завдання, яке показано на рисунку 3.3.5.

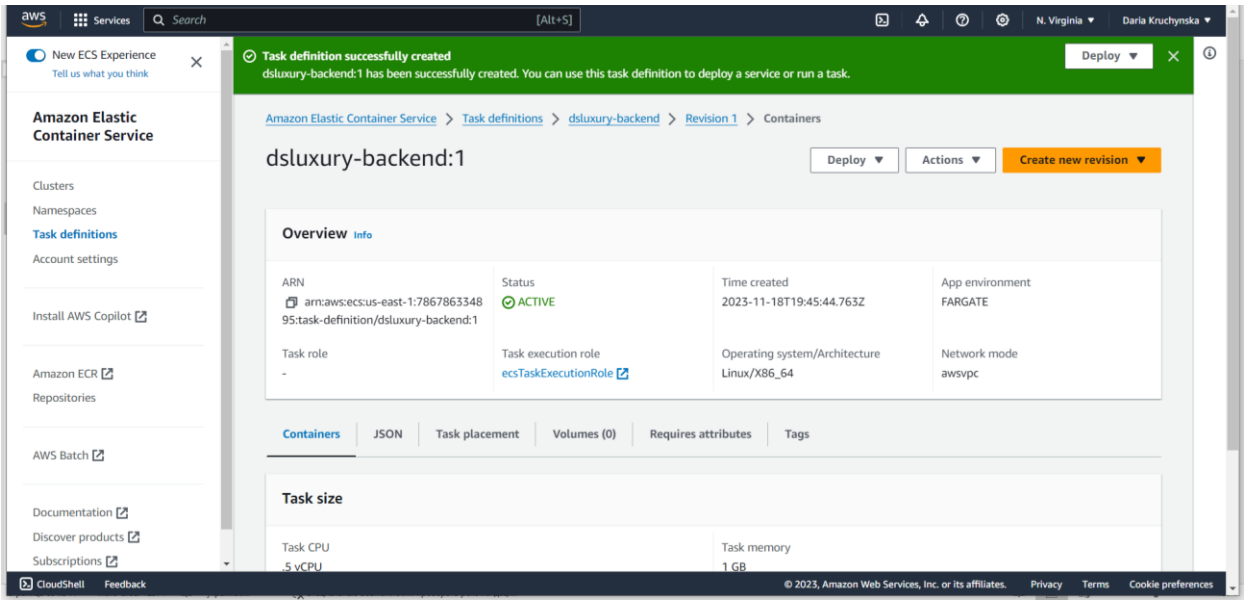

Рисунок 3.3.5 – Успішно створене завдання для серверної частини

Завдання та кластер створені для серверної частини, тому далі необхідно запустити завдання, яке відображається на рисунку 3.3.5. Так як вже створено кластер та завдання, тепер у створеному кластері необхідно запустити створене завдання, яке на рисунку 3.3.5. Початок запуску завдання аналогічний як на рисунку 3.2.9. Далі потрібно налаштувати параметри для запуску завдання, для початку параметри обчислень, для даного завдання,

запуск буде без використання стратегій постачальника потужностей, яка реалізована на рисунку 3.3.6.

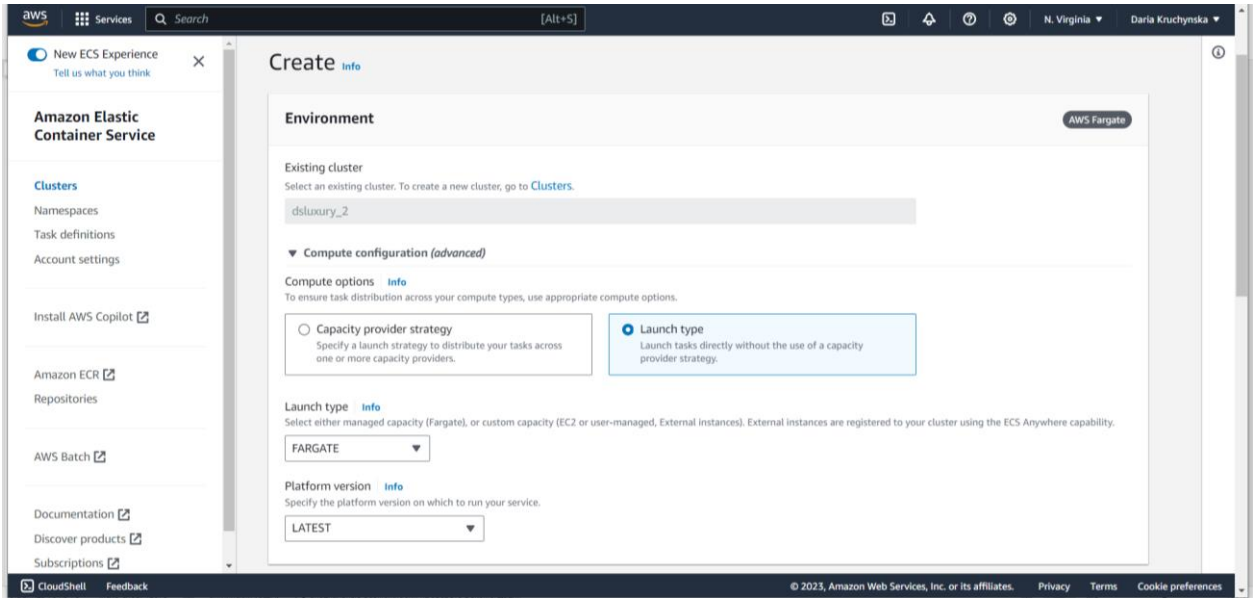

Рисунок 3.3.6 – Обрання параметрів обчислення для серверної частини

Після налаштувань параметрів обчислення, налаштовується конфігурація розгортання на рисунку 3.3.7, відповідно розгортається завдання для серверної частини.

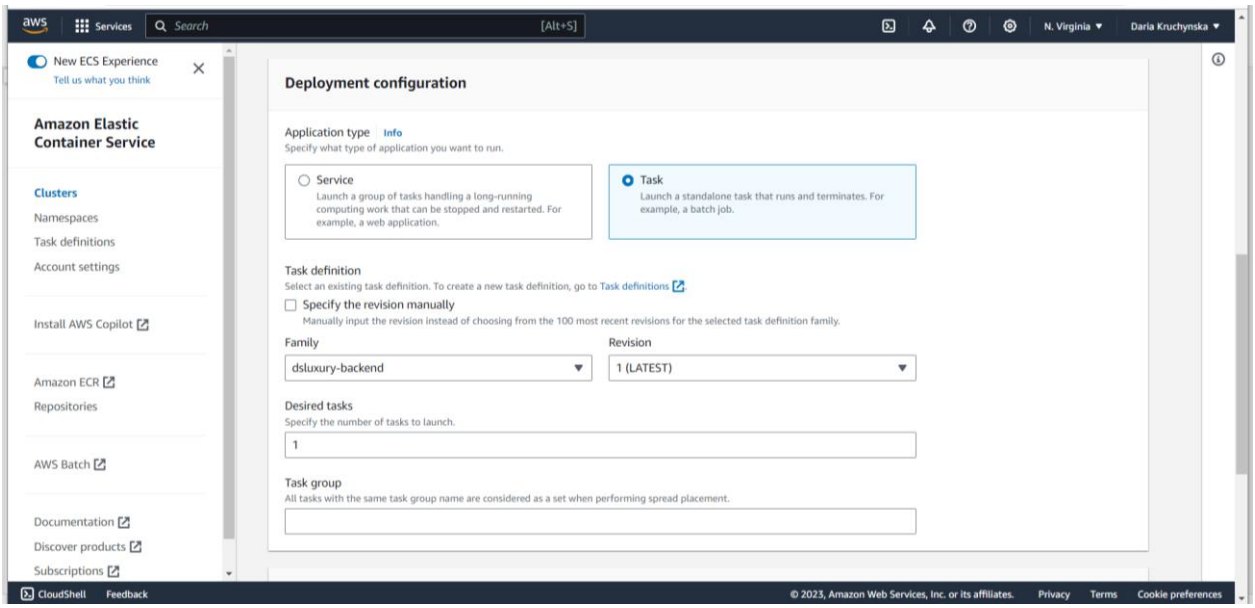

Рисунок 3.3.7 – Налаштування конфігурації розгортання для серверної частини

Після цього налаштовуються параметри мережі, де саме буде запускатись завдання, які аналогічні до рисунка 3.2.12 для завдання клієнтської частини.

Всі налаштування завершені, тому необхідно запустити завдання для серверної частини.

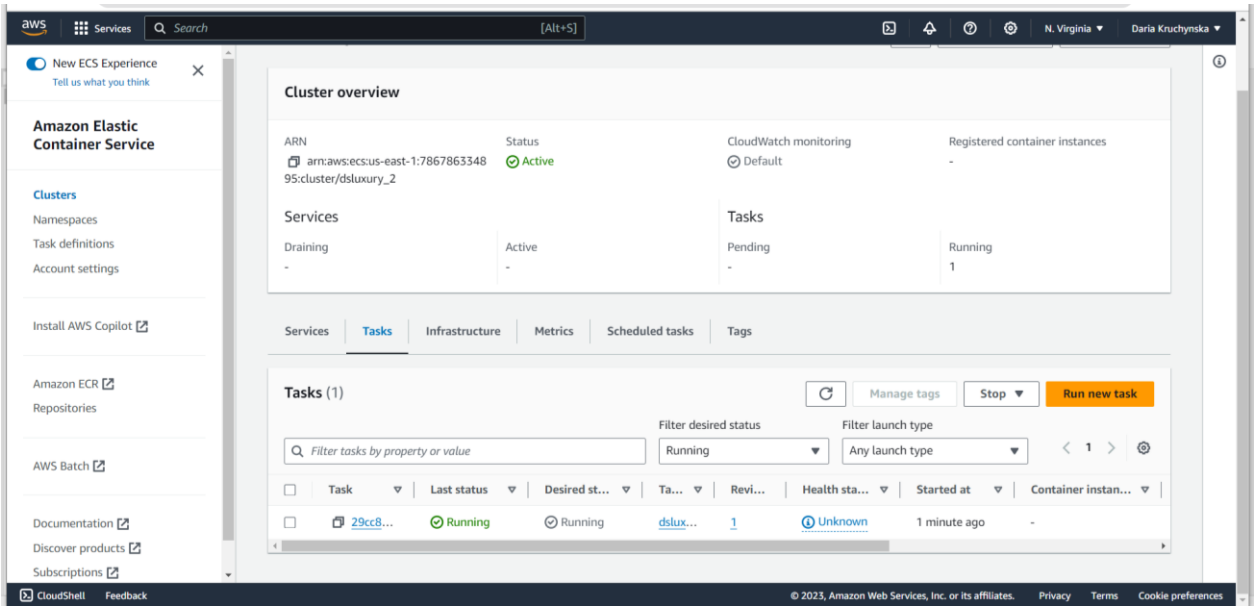

Рисунок 3.3.8 – Успішно запущене завдання у кластері для серверної частини

Далі розгортаючи серверну частину хмарної інфраструктури, налаштовується сервіс AWS Lambda, використовуючи який запускаються відповідні функції, які потрібні для інтернет-магазину. Функції які можна створити та запустити є різноманітні й звичайно, що усі вони реалізовуються під конкретний магазин. Тому на даному етапі розробки розгортання конкретних функцій не є доречним. Але звичайно, що можна налаштувати та запустити саму функцію, яка у майбутньому може бути відредагована під конкретний магазин.

Взагалі AWS Lambda працює з великою кількістю інших сервісів, що дозволяє реалізувати різноманітні функції в залежності від потреб. Даний сервіс автоматично буде запускати потрібний програмний код, тобто функцію, у відповідь на різноманітні ситуації. Наприклад, це може бути оновлення таблиць, які створені в Amazon DynamoDB, або ж це будуть відповіді на HTTP-запити через сервіс Amazon API Gateway тощо. Для початку необхідно створити функцію нажавши відповідну кнопку, як на рисунок 3.3.9.

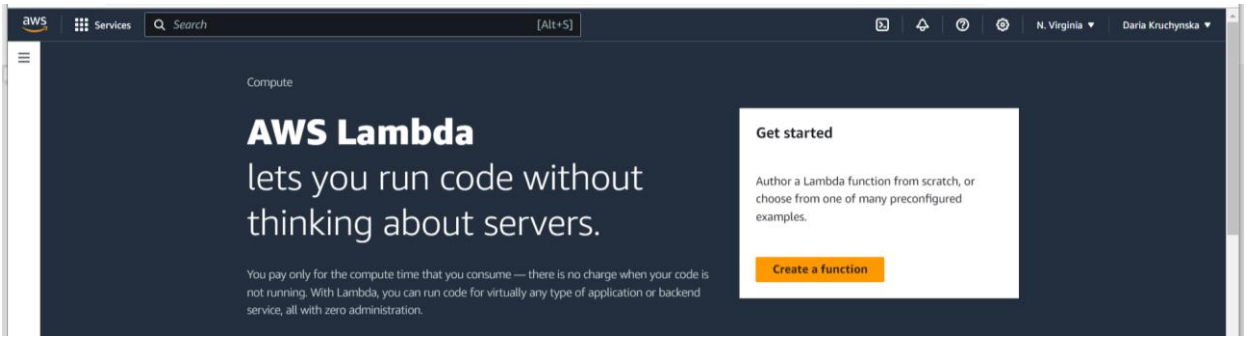

Рисунок 3.3.9 – Створення функції для серверної частини

Далі налаштовується сама функція, як показано на рисунку 3.3.10. Спочатку обирається стратегія розробки функції, на даному етапі підходить використання вже створених функцій, які підійдуть в майбутньому під будь-який інтернет-магазин, з мінімальним внесенням корективів під потреби. На даному етапі створюється функція для взаємодії з таблицею сервісу DynamoDB, яка являє собою серверний інтерфейс читання та запису в DynamoDB з використанням Amazon API Gateway з кінцевою точкою RESTful API та реалізована на python3.10.

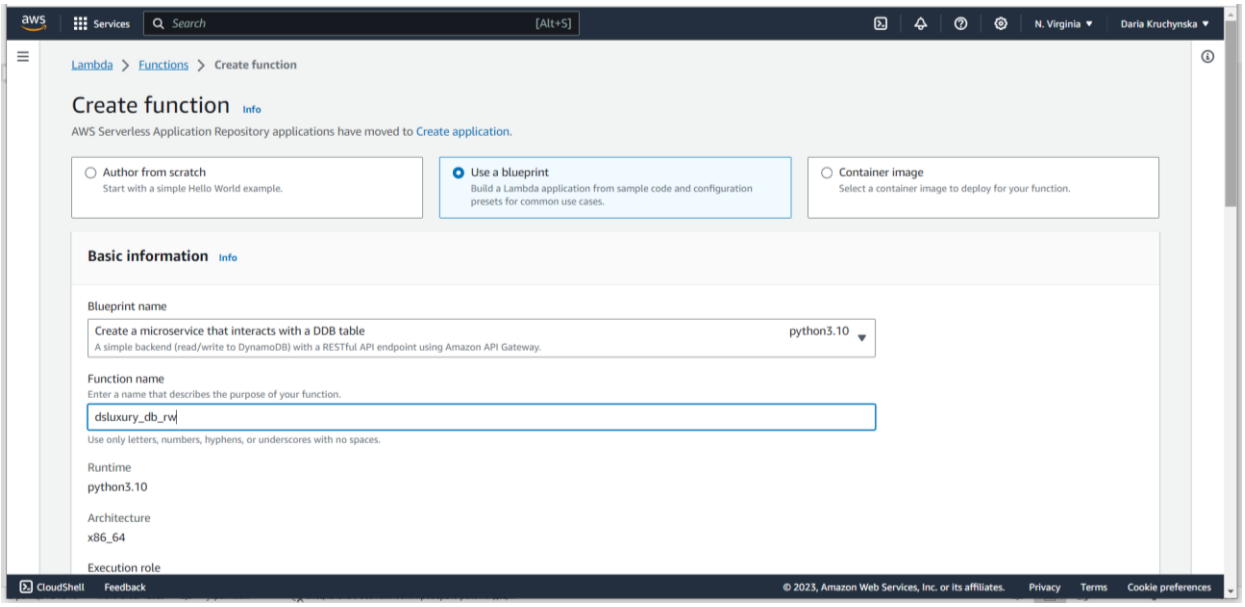

Рисунок 3.3.10 – Налаштування функції читання та запису таблиць БД для серверної частини

Далі створюється нова роль, яка буде визначати дозволи для даної функції, надається логічна назва, як на рисунку 3.3.11.

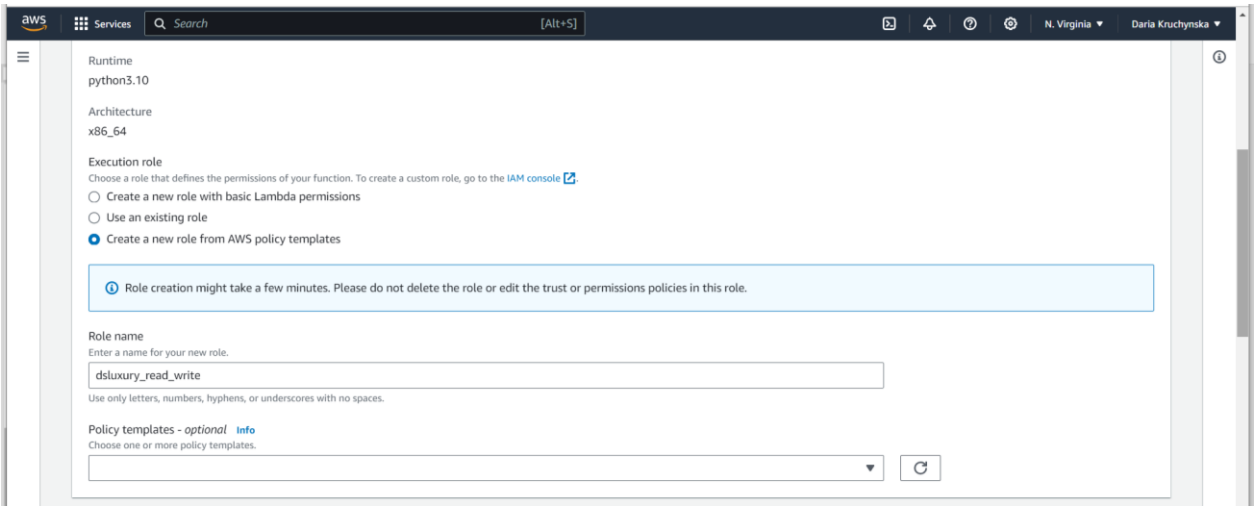

Рисунок 3.3.11 – Налаштування ролей для функції dsluxury_db_rw

Після всіх налаштувань створюється для зручності API шлюз, як показано на рисунку 3.3.12. Обирається тип API, для зручності це REST API, при використанні якого отримується повний контроль над запитами та відповідями, та можливість управління ними, що є дуже зручним.

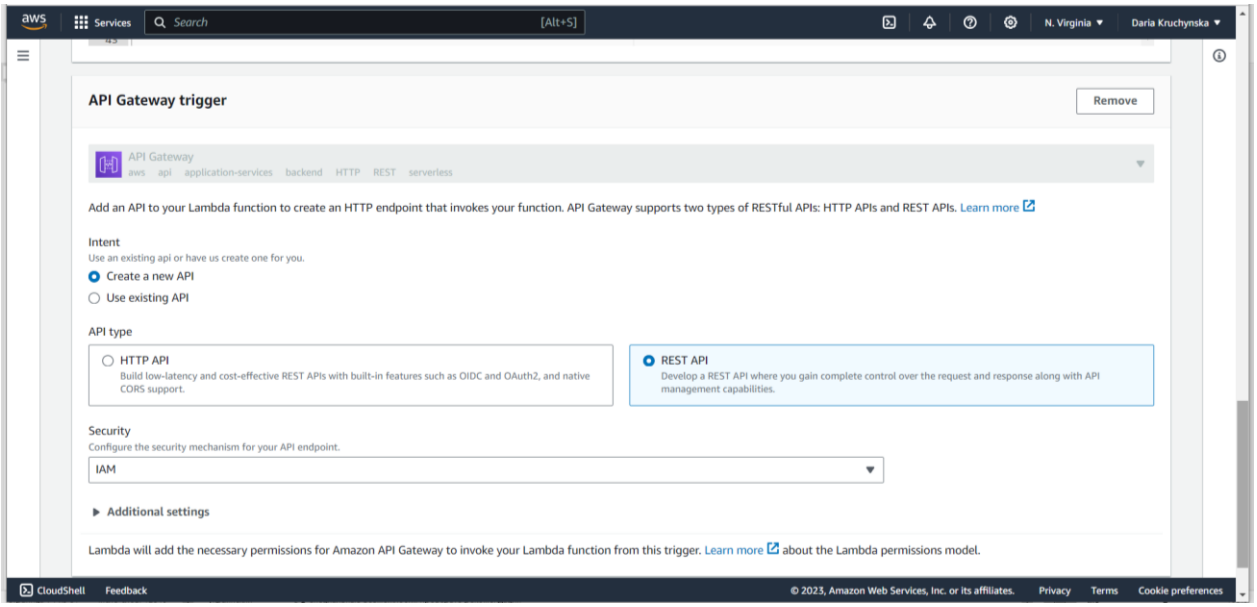

Рисунок 3.3.12 – Створення API для функції dsluxury_db_rw

Після усіх налаштувань, отримуємо створену функцію dsluxury_db_rw з API, яка на рисунку 3.3.13 та можливостями управляння, редагування і т.д. під потребу. Можна додати ще й інші функції, але на даному етапі цього достатньо. Інші функції будуть додано у майбутньому процесі розробки проєкту.

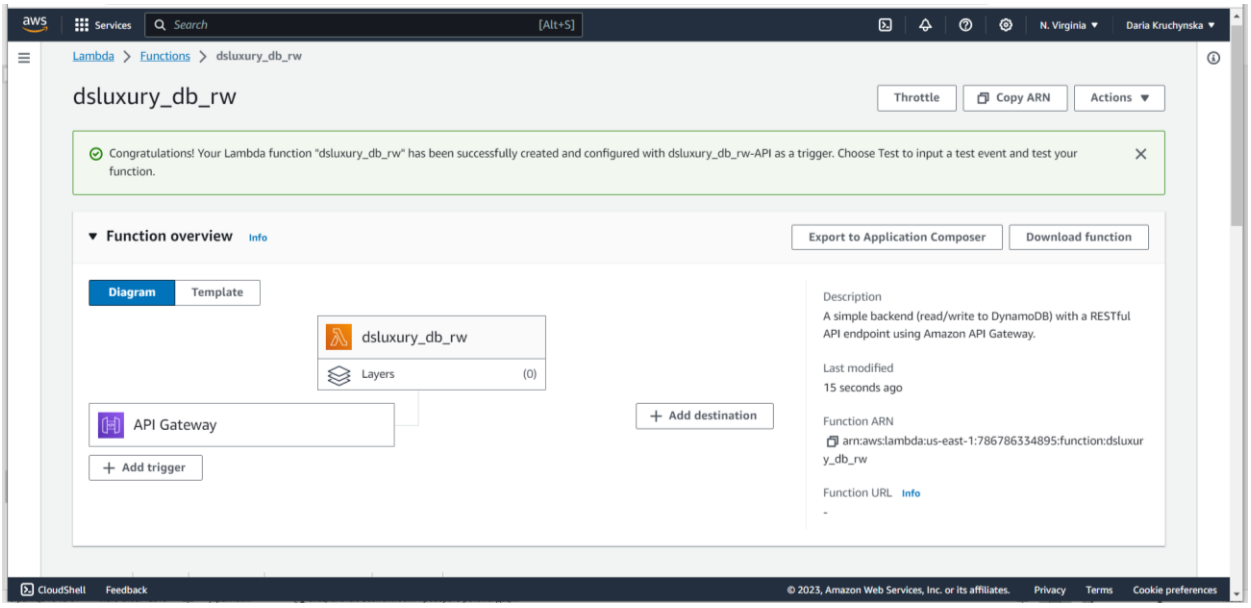

Рисунок 3.3.13 – Успішно створена функція dsluxury_db_rw API з Gateway

Як вже зазначалось у розділі 3.2 при реалізації клієнтської частини, що майже усі додатки повинні мати БД. Так як розробка БД вже почалась у клієнтській частині, то у серверній вона продовжиться та доповниться новими таблицями потрібними для серверної частини. Для цього аналогічно використовується сервіс Amazon DynamoDB, про який більш детально описано в розділі 3.2.

Саме використання сервісу DynamoDB, на серверному рівні буде забезпечувати також інтернет-магазин сховищем даних, який буде містити клієнтів, відповідно товари та дані транзакцій клієнтів, які можуть бути даними про кошик, або ж замовлення тощо.

Усі етапи створення таблиць повторюються як на рисунках 3.2.20 – 3.2.22, тому їх демонстрація в даному розділі відсутня. Таблиця користувача, яка успішно створена на рисунку 3.2.23, буде використовуватись і в серверній частині. Далі створюються таблиці для серверної частини, які відображені на рисунку 3.3.14, такі як замовлення, оплата, товар, рахунок, склад та виправляння, які мають логічні назви та підійдуть під будь-який інтернет-магазин.

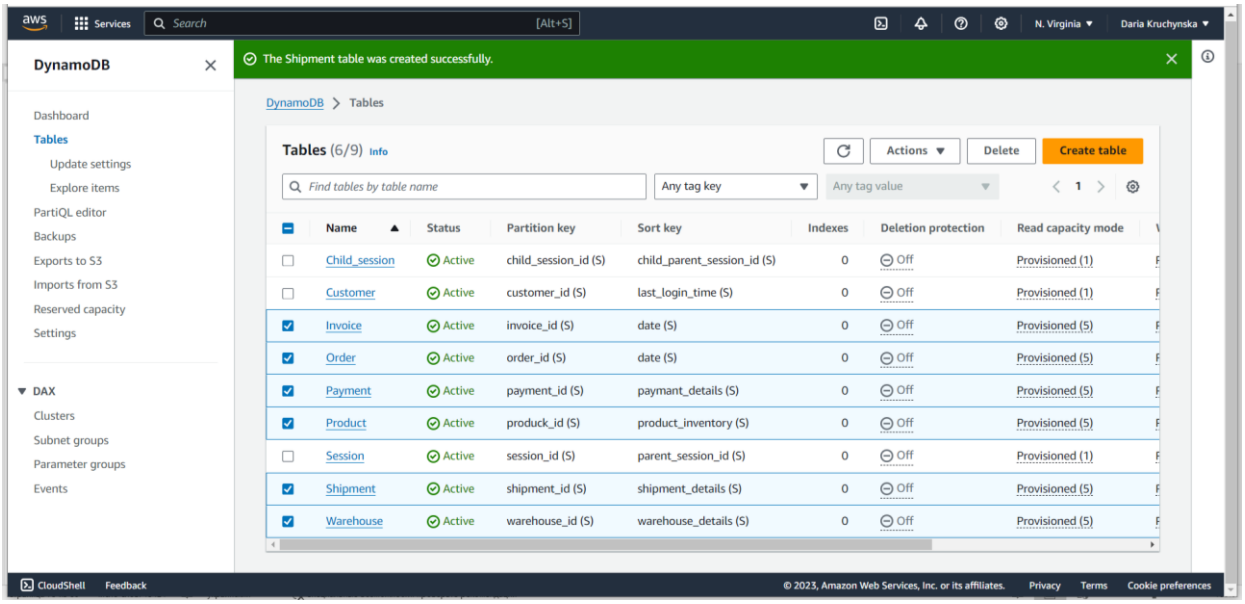

Рисунок 3.3.14 – Успішно створені таблиці “Invoice”, “Order”, “Payment”, “Product”, “Shipment”, “Warehouse” БД для серверної частини

Далі у серверній частині проєкту необхідно розгорнути як і в клієнтській частині сервіс ***Amazon ElastiCache,*** який буде кешувати вже трансформовані відповіді окремих мікросервісів, які розгорнуті. Більше детально описано можливості сервісу Amazon ElastiCache у розділі 3.2. Початок роботи з даним сервісом повторюється як на рисунку 3.2.14 та обране сховище даних не змінюється, а залишається Redis як і в клієнтській частині. Метод створення кластера та обрання конфігурації повторюється як на рисунку 3.2.15. Після цього необхідно ввести назву та опис кластера для серверної частини, як на рисунку 3.3.15.

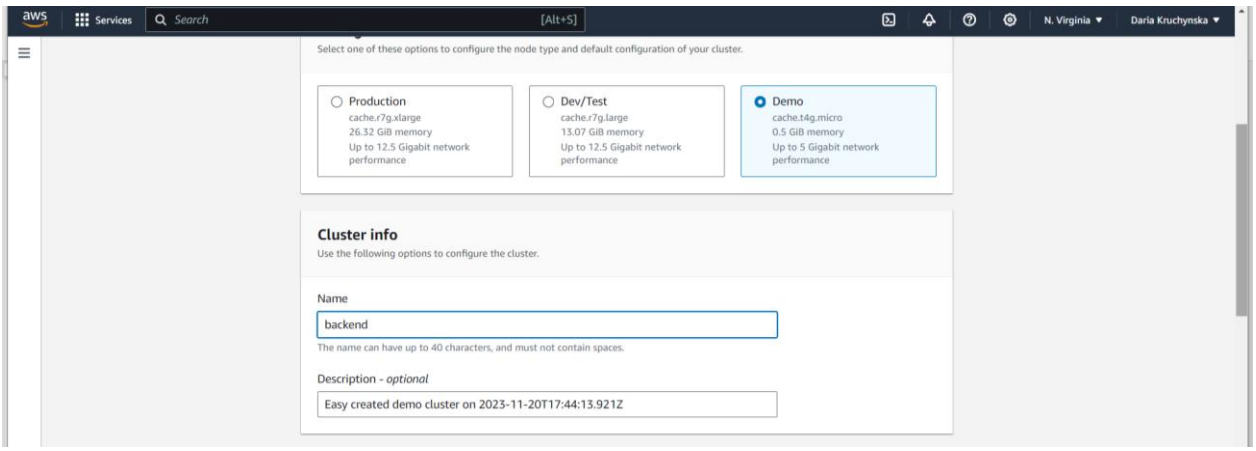

Рисунок 3.3.15 – Налаштування інформації про кластер для серверної частини

Далі як і при налаштуванні кластера в клієнтській частині, необхідно налаштувати параметри мережевого зв’язку та створити нову групу зв'язку з відповідною інформацією про неї, продемонстровано на рисунку 3.3.16.

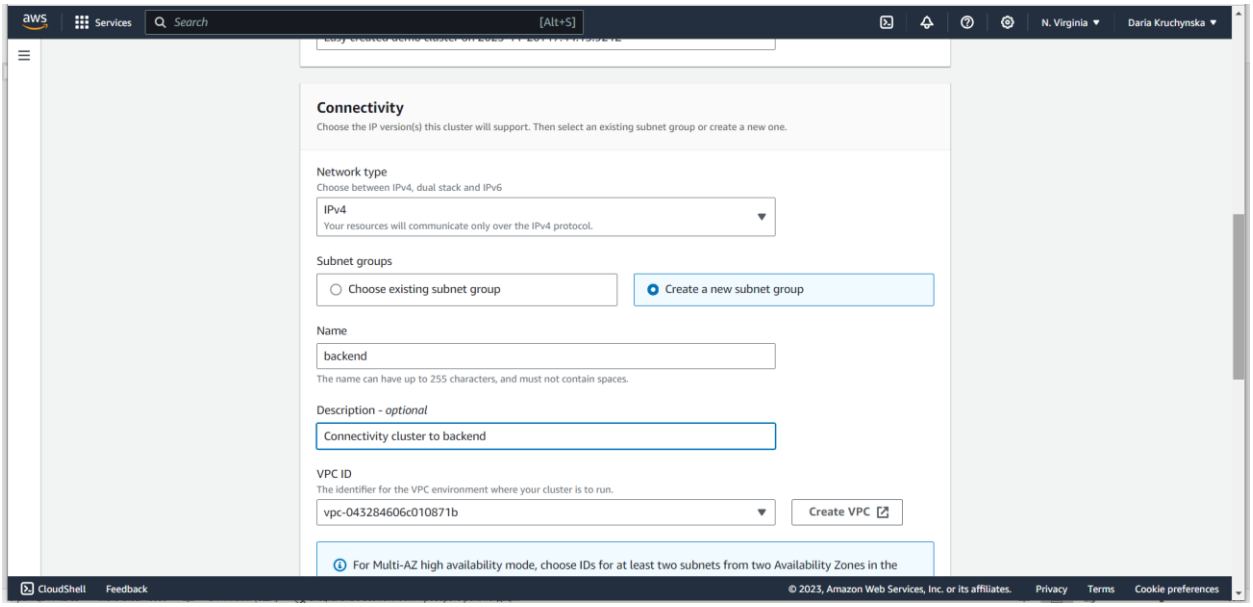

Рисунок 3.3.16 – Налаштування мережевого зв’язку з кластером для серверної частини

Далі для створеної групи необхідно налаштувати підмережі, як на рисунку 3.3.17, для зон доступності.

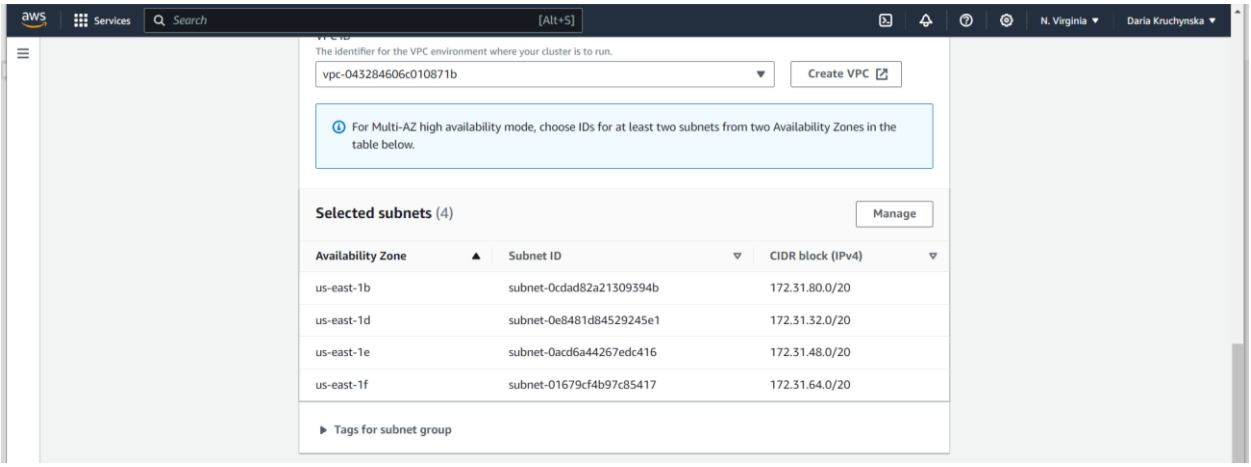

Рисунок 3.3.17 – Налаштування підмереж у зонах доступності для серверної частини

Після всіх налаштувань, можна створити кластер, який буде виконувати кешування даних у серверній частині, як на рисунку 3.3.18.

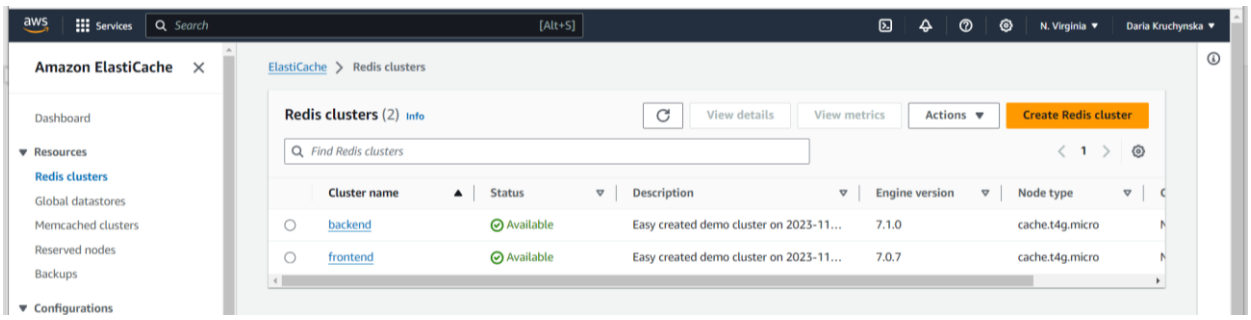

Рисунок 3.3.18 – Успішно створений кластер для кешування даних у серверній частині

3.4 Розгортання серверів системи захисту

Кожна система, додаток, інфраструктура тощо, потребує захисту інформації та самої системи. Звичайно що існують методи, засоби і т.д., захисту як інформації, так і самих програмних продуктів і не тільки. Адже з винайденням нових методів захисту, з'являються і нові загрози, тому цей процес циклічний та невід'ємний.

Важливо зазначити, що які б заходи безпеки не були реалізовані, все одно система може мати вразливі місця. Задача експерта в галузі кібербезпеки, реалізувати заходи безпеки, аби максимально захистити систему на стільки, на скільки це можливо. Або ж, що найменше, захистити програмний продукт так, щоб навіть у випадку загроз, яких існує безліч, можливо було швидко виявити їх та виконати профілактику тощо.

Безпека в хмарі завжди мала спірні питання та твердження і звичайно, що і сьогодні це залишається актуальним питанням. Звичайним фактором проблем безпеки в хмарі є попит саме на хмарні сервіси який зростає з кожним днем. Оскільки велика кількість інформації, даних, цілих інфраструктур переноситься у хмару, а саме це в більшості випадків цікавить зловмисників, це змушує їх вигадувати все нові й нові методи заволодіння цих даних, або ж цілою хмарною інфраструктурою компанії тощо.

Важливою складовою безпеки у хмарі й взагалі будь-якої системи, залишається людина, тобто користувач. Адже у значній частині проблем із безпекою, головним фактором небезпеки стає користувач, а саме його

неуважність, яка зумовлює, чи то навмисну шкоду, або ж випадкову. Навіть не зважаючи на те, що за весь час існування хмарних технологій, ще не виникало глобальних проблем із доступність даних та їх безпекою, це не дає повної впевненості у безпеці в майбутньому.

На сьогодні найсвіжіша стаття від Cloud Security Alliance, яка вийшла в листопаді цього року, в якій було висвітлено нову матрицю загроз у хмарі для галузевого співробітництва. Аналізуючи дану статтю, одна з основних проблем є проблема швидкості розвитку технологій та нових послуг які пропонуються, хоча це є і плюсом одночасно. Але саме для безпеки у хмарі, дана проблема спонукає до відставання в знаннях та вирішеннях нових загроз, та відповідно несвоєчасного винайдення нових рішень безпеки. [23] Звичайно це не одна проблема безпеки у хмарі, але вона важлива.

Минулого року був щорічний рейтинг Cloud Security Alliance, у якому представили 11 загроз безпеки. На сьогодні так і залишилось те, що зловмисники більше уваги приділяють саме кінцевому споживачу, адже вони мають вразливість. Всі представлені проблеми є досі актуальними. [19]

Цього року в середині осені вийшла нова стаття, яка базувалась саме на торішній. [26] В новій статі спираючись на минулі дослідження та аналізуючи 11 загроз безпеки, було реалізовано моделі загроз на кожну загрозу та відповідно зроблено висновки та винесено рекомендації. [24] Тому такі проблеми безпеки потрібно враховувати та аналізувати не тільки розробникам та спеціалістам безпеки, а й користувачам.

Взагалі сервіси захисту AWS налічують достатню кількість, вони розглядались в розділі 2.2 більш детально. Головним недоліком всіх цих сервісів є те, що всі вони мають ціну, яка коливається від мінімуму до більших цін. Звичайно перевагою є те, що в більшості випадків ціна знімається тільки при використанні, але для навчального проєкту деякі сервіси за ціною просто перевищують бюджет проєкту.

Найкращим варіантом для даної інфраструктури було б використати сервіс ***AWS Firewall Manager,*** який являє собою брандмауер, тобто

міжмережевий екран. Даний сервіс комунікує з сервісом AWS Config, який був розгорнутий у розділі 3.1, тому його використання було б доцільним та зручним, але ціна даного сервісу 100$ в місяць, які бюджет проєкту покрити не можуть. При взаємодії з даним сервісом кожний обліковий запис користувача та ресурси були б захищені.

AWS Firewall Manager зі сторони безпеки більше націлений на безпеку між довіреною мережею та невідомою, тобто стає між ними стіною. Тому виходячи із ціни на сервіс, можна було б використати інший сервіс ***AWS WAF***, який також являється брандмауером, але має відмінність. Даний сервіс націлений більше на веб-додатки та використовується для моніторингу, перегляду даних, блокування трафіку який іде із додатка, або ж до нього та захищає від різноманітних експлойтів та ботів.

Найголовніше, що він захищає від веб-атак, а саме від DDOS-атак та шкідливого трафіку тощо, так як підтримує більш як сто правил безпеки та при цьому з мінімальною затримкою трафіку. Цей сервіс також потребує витрат, але ця ціна помірна. Тому для даного проєкту доцільно реалізувати саме його. Початок роботи із сервісом AWS WAF починається зі створення веб ACL, тобто списку правил для керування безпекою. Для початку необхідно натиснути відповідно кнопку, як на рисунку 3.4.1.

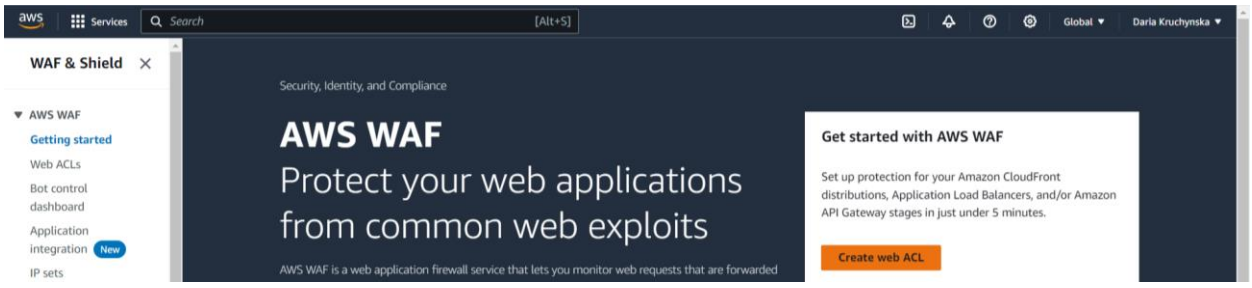

Рисунок 3.4.1 – Створення правил безпеки

Створення ACL листів проходить у 5 етапів. ***На першому етапі*** необхідно описати веб-список керування доступом та пов’язати його із відповідними ресурсами AWS, які були створені раніше та будуть взаємодіяти зі створеними правилами, як на рисунку 3.4.2.

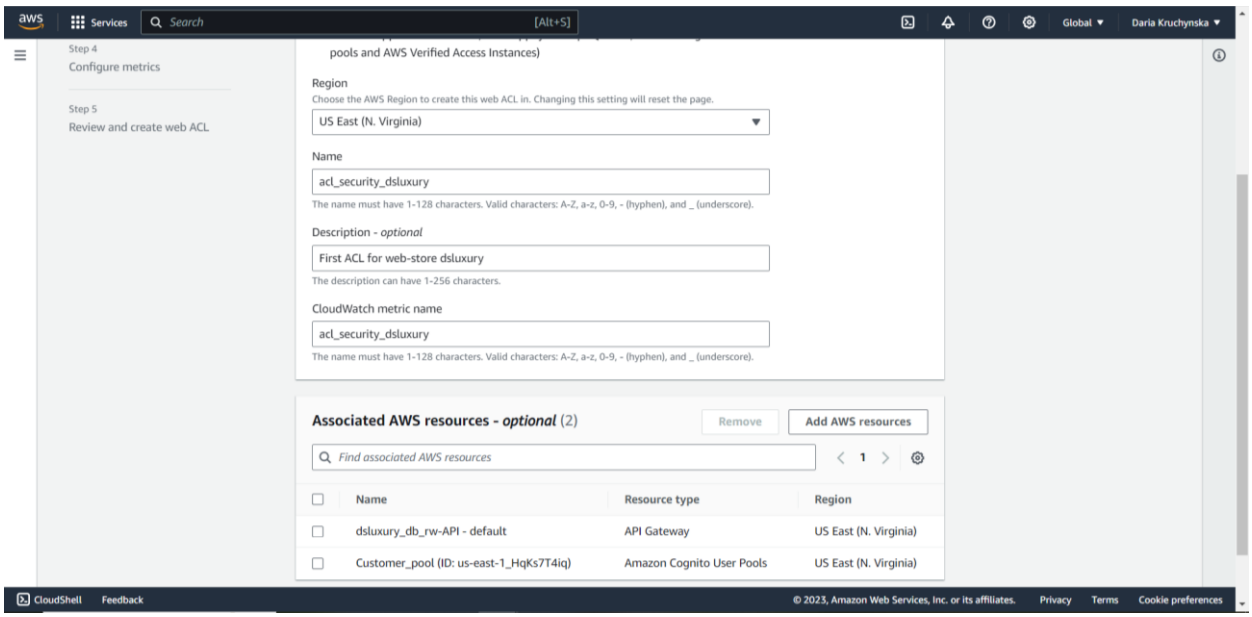

Рисунок 3.4.2 – Перший етап створення ACL правил

Далі переходимо ***на другий етап***, в якому створюються правила та групи правил. В даному випадку правило є шаблоном атаки, яку слід шукати у веб-запитах та діями які потім виконуються, якщо запит відповідає шаблону. Групи ж правил є наборами правил, які багаторазово використовуються. В нашому випадку буде набір основних правил, який містить правила, які зазвичай застосовуються саме до веб-застосунків, його реалізація показана на рисунку 3.4.3.

Дане правило забезпечить захист від використання широкого спектра вразливостей. Цього буде достатньо на даному етапі, так як за кожне правило знімаються кошти. Також налаштовано, що за замовчуванням будуть пропускатись лише ті запити, які не заборонені вище зазначеним правилом.

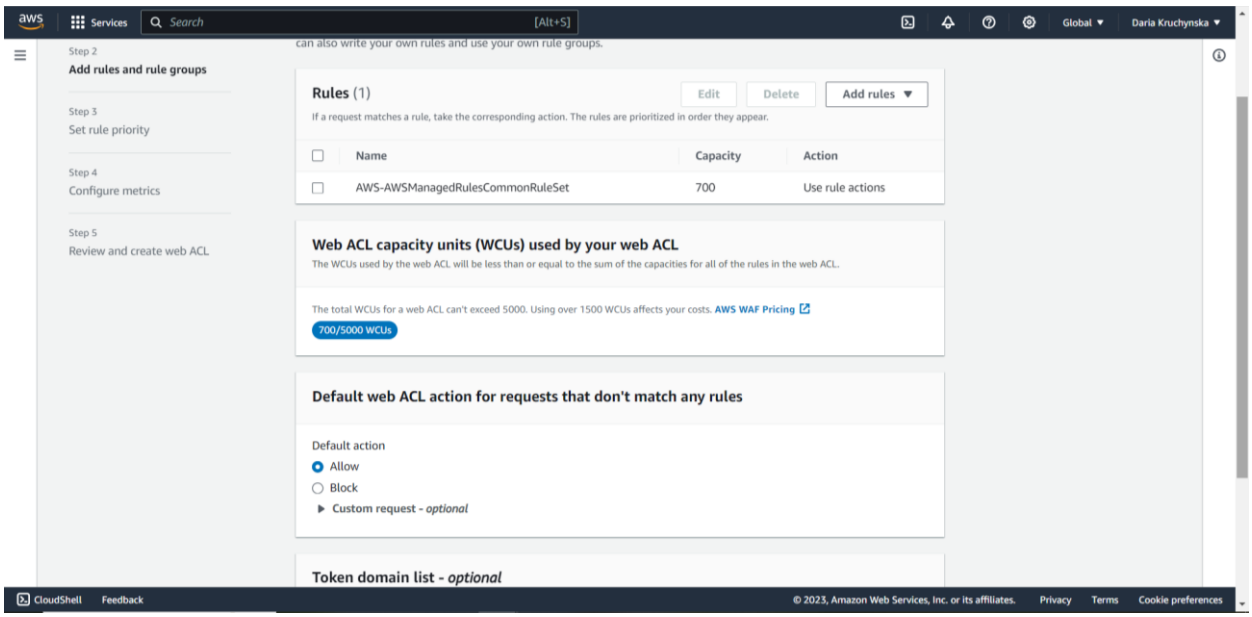

Рисунок 3.4.3 – Другий етап створення ACL правил

Після цього ***на третьому етапі*** встановлюється пріорітет правил, як на рисунку 3.4.4, але так як в нас тільки одне правило, то відповідно пріорітет не потрібний.

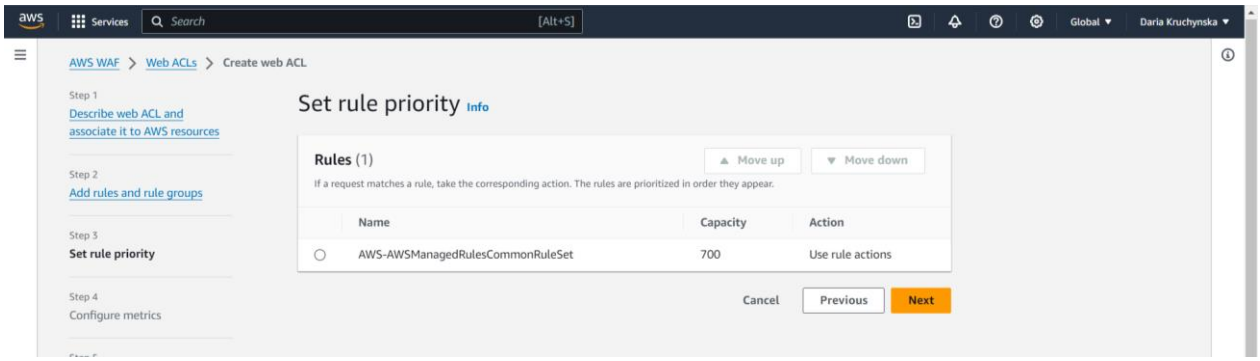

Рисунок 3.4.4 – Третій етап створення ACL правил

На четвертому етапі налаштовуються показними метрик, на даному етапі розробки доцільно залишити налаштування за замовчуванням, як на рисунку 3.4.5.

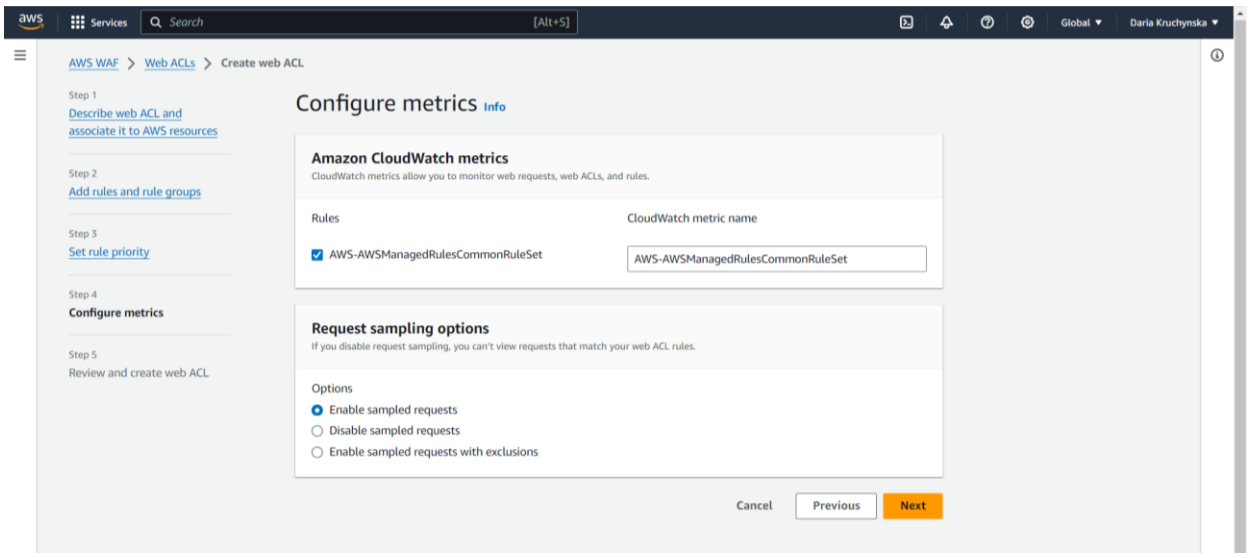

Рисунок 3.4.5 – Четвертий етап створення ACL правил

На останьому, тобто ***п'ятому етапі*** відбувається перевірка створених ACL правил, як на рисунку 3.4.6, та відповідно редагування за потреби.

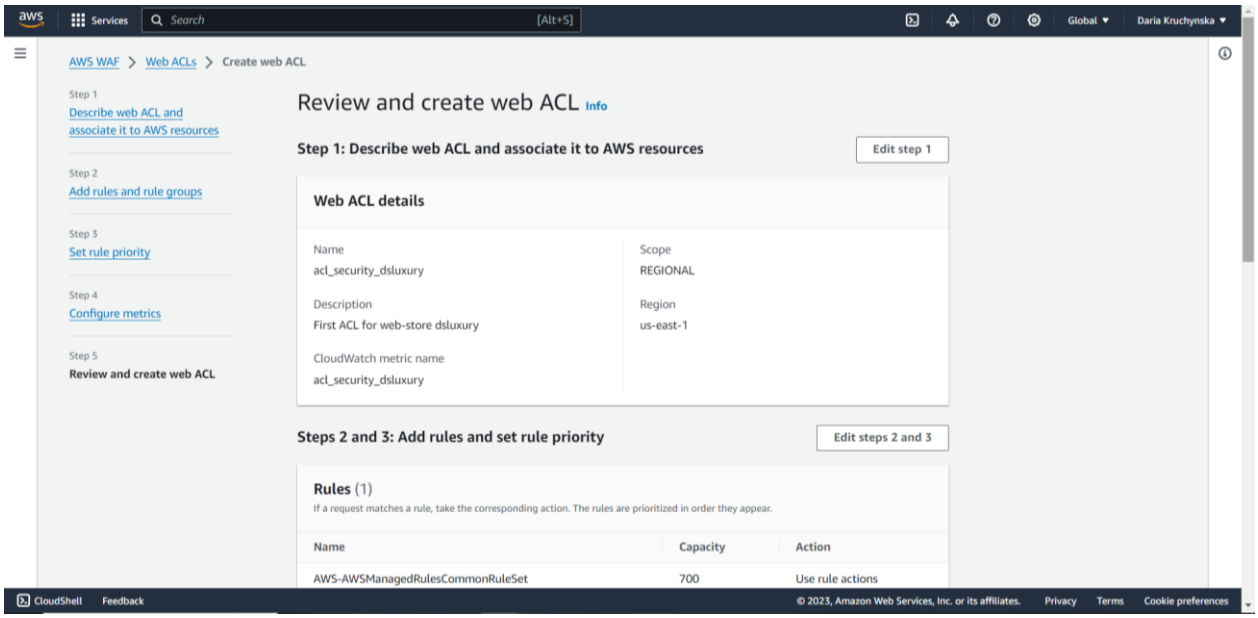

Рисунок 3.4.6 – П'ятий етап створення ACL правил

І в кінцевому результаті, коли всі перевірки виконано та відредаговано за потреби, створюється ACL правило, як на рисунку 3.4.7.

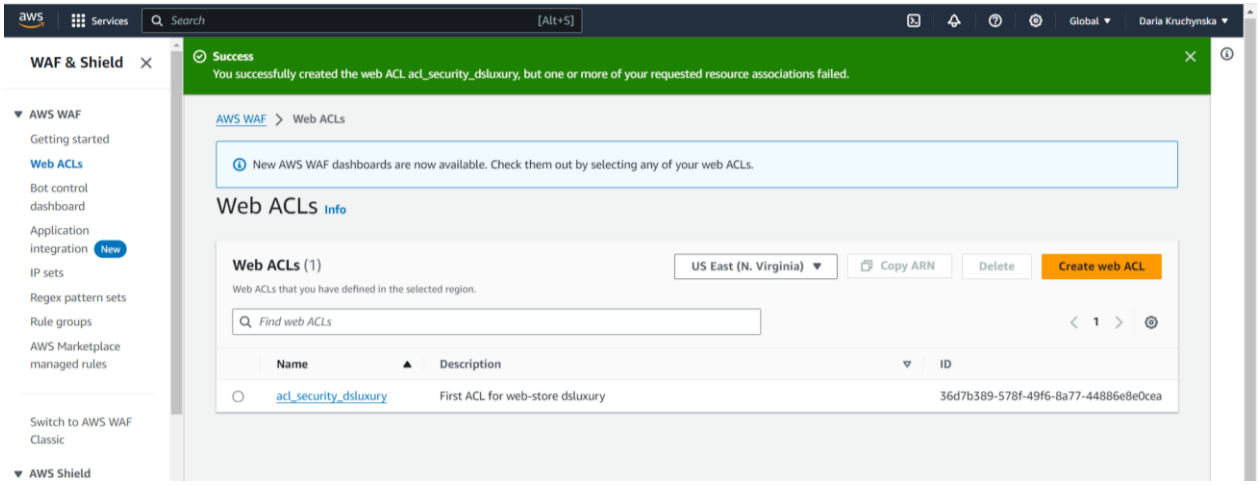

Рисунок 3.4.7 – Успішно створене ACL правило

Також до сервісів безпеки можна віднести сервіс ***AWS Cognito***, який розгортався в розділі 3.1, так як він також робить перевірку, оцінку та аналіз конфігурацій, саме своїх ресурсів. Тому для даної хмарної інфраструктури та на цьому етапі, реалізованого захисту буде достатньо. При майбутній розробці цей список можна буде розширити, але все буде базуватись на бюджеті проєкту, адже всі сервіси безпеки мають свої тарифи оплати.

3.5 Розгортання комерційної частини інфраструктури

Комерційна інфраструктура, або ж іншими словами електронна комерція, надає велику кількість можливостей для бізнесу. Інтернет-магазини напряму пов’язані із комерцією, тому звичайно сервіси, які будуть розгортатись, є важливими для полегшення та покращення веб-сервісу загалом.

Вибір сервісів для розгортання комерційної інфраструктури на пряму пов’язаний із потребами самого магазину та бюджетом, це також не мало важливий фактор. Звичайно можна реалізувати максимальний функціонал за допомогою AWS сервісів, але не завжди велика кількість функціонала покращує сам продукт. Адже у різноманітті послуг та можливостей, клієнт може втратити увагу та взагалі перейти в інший магазин. Тому повинен бути звичайно баланс.

Для комерційної інфраструктури обрано сервіс ***Amazon Open Search,*** який буде використовуватись для логічного пошуку та виконання фільтрації товарів тощо. Взагалі логіка даного сервісу полягає у простому розгортані та масштабуванні кластерів, які в подальшому легко експлуатуються у хмарі. При створенні кластерів обирається пошукова система. ***OpenSearch*** є аналітичною та пошуковою системою, яка використовується як раз для моніторингу додатка в реальному часі, аналізу журналів й моделей поведінки користувачів додатка.

Для початку використання даного сервісу необхідно створити домен, як на рисунку 3.5.1, обравши відповідний варіант, який буде еквівалентний кластеру. В нашому випадку системи, розгортається захищений кластер.

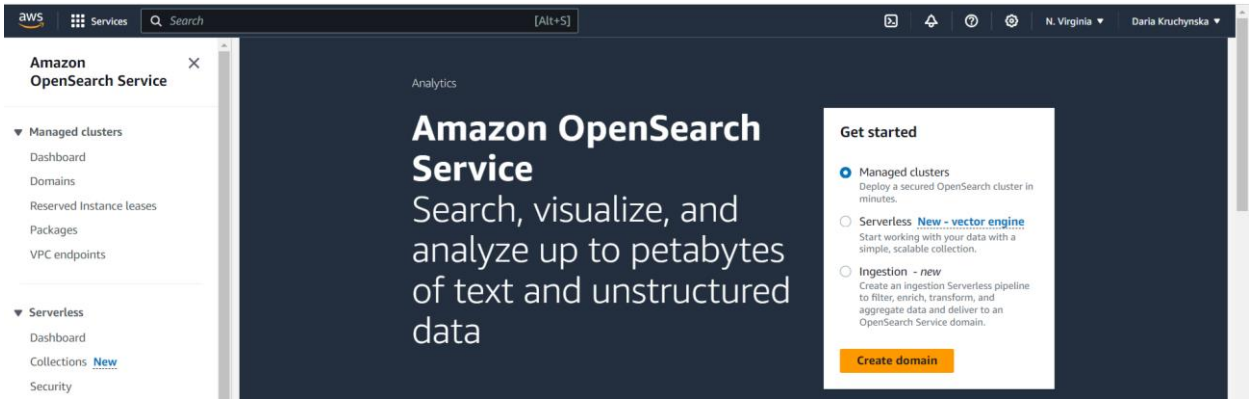

Рисунок 3.5.1 – Розгортання захищеного кластера для OpenSearch

Далі налаштовується сам домен, як на рисунку 3.5.2, необхідно надати логічну назву домену, метод створення його та версію OpenSearch. На даному етапі розробки краще обрати легкий спосіб створення домену, а не стандартний. Оскільки, в майбутньому можна буде внести корективи під конкретні потреби, які в залежності від характеристик є платними. Але тих налаштувань які є зараз буде достатньо для даної хмарної інфраструктури.

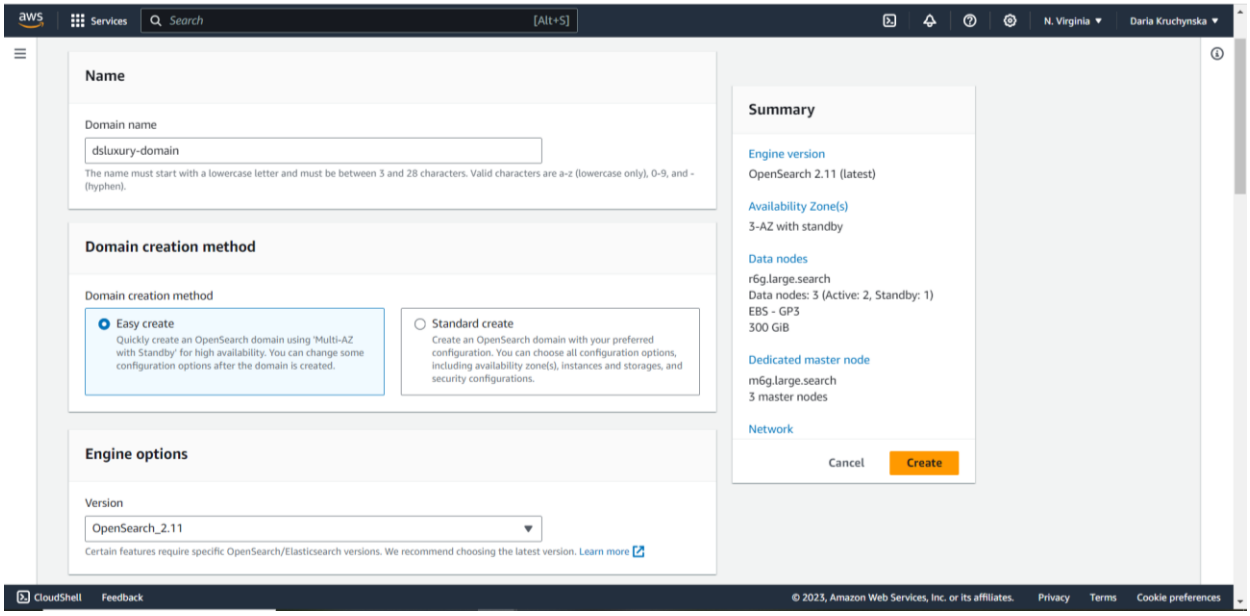

Рисунок 3.5.2 – Налаштування домену dsluxury-domain

Далі необхідно налаштувати параметри мережі, як на рисунку 3.5.3. На даному етапі буде налаштований публічний доступ, так як за використання VPC доступу знімаються кошти з рахунку. Але публічний доступ не є безпечним, тому в кінцевому налаштуванні проєкту він буде змінений на VPC доступ та доналаштований.

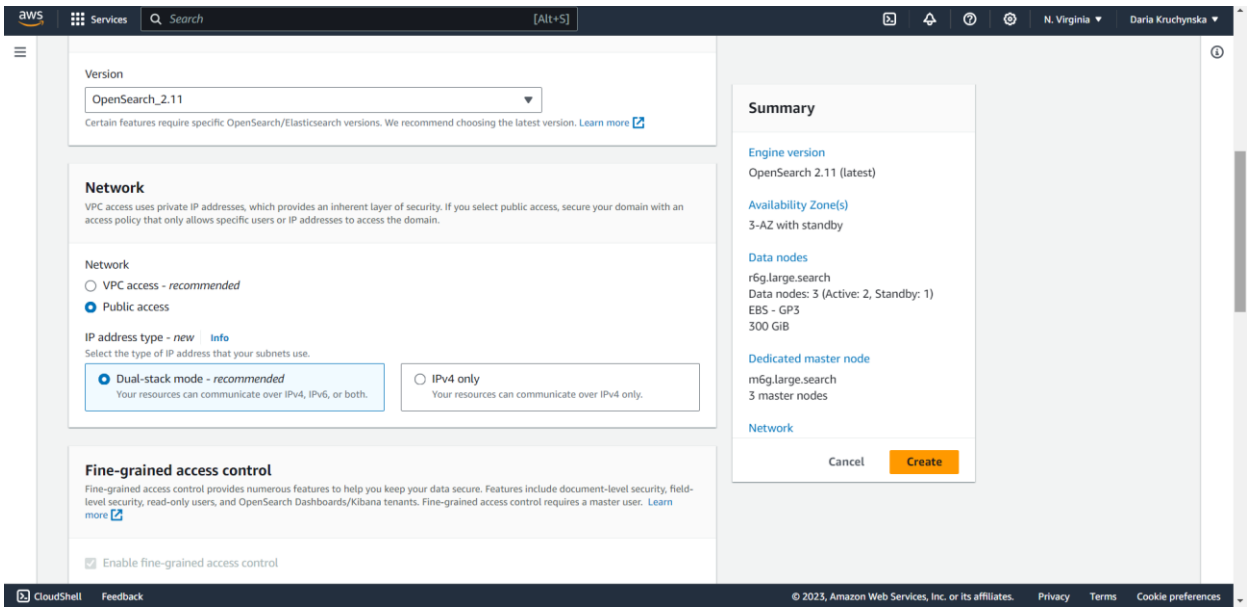

Рисунок 3.5.3 – Налаштування параметрів мережі

Після налаштувань параметрів мережі, необхідно налаштувати параметри доступу. Так як керування доступом надає численні можливості для захищеності даних, що є важливим. Для цього на рисунку 3.5.4, створено головного користувача з ім’ям та паролем. Дані можливості надають безпеку

на багатьох рівнях, таких як рівень документів, полів, управлінням доступом тощо.

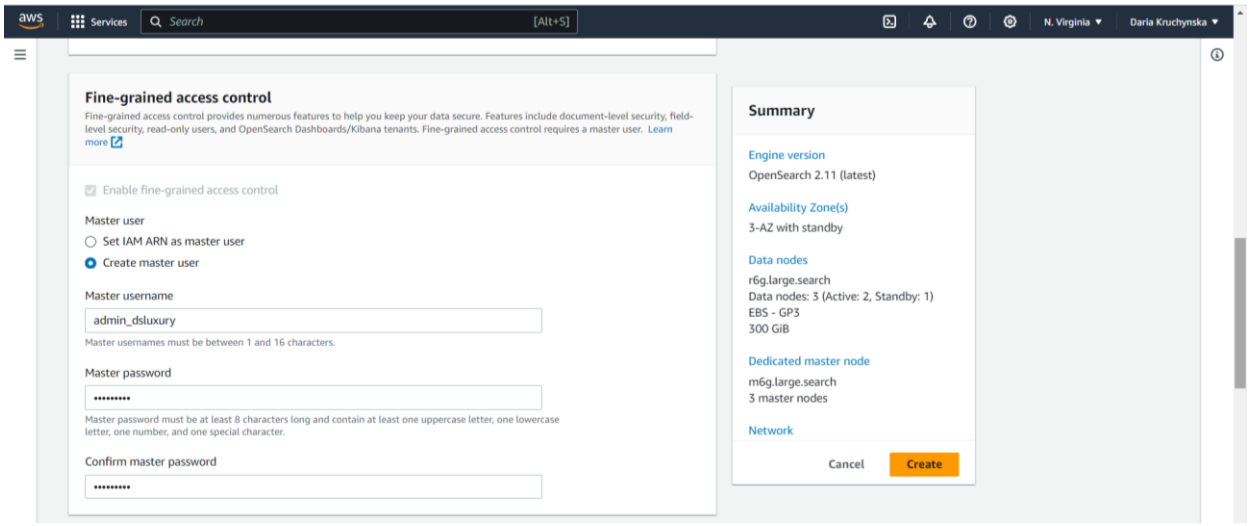

Рисунок 3.5.4 – Створення головного користувача для керуванням доступом

Після всіх налаштувань створюється домен, як на рисунку 3.5.5, який в майбутньому можна буде відредагувати, або ж якщо налаштовані параметри влаштовують та відповідають потребам, то так і залишити.

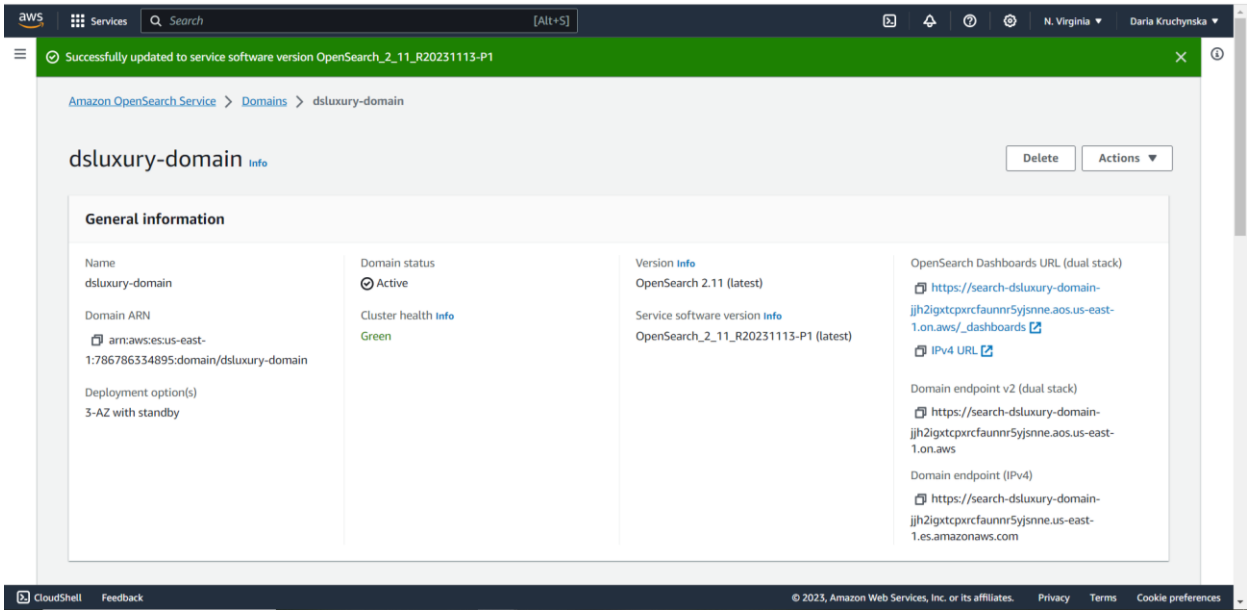

Рисунок 3.5.5 – Успішно створений домен для OpenSearch

Наступний сервіс, який буде налаштовуватись для комерційної частини, це ***Amazon Location Service.*** Розгорнувши даний сервіс, можна додати інформацію в веб-додаток про місцезнаходження, що є актуальним. Так як більшість клієнтів цікавиться, де саме знаходиться інтернет-магазин, та для

розуміння звідки буде доставлення товарів. Або ж для перегляду локальних магазинів, якщо вони наявні.

Даний сервіс є зручним для інтернет-магазину і не тільки, так як, наприклад, за допомогою інформації, яка отримується, через нього можна організувати доставлення товарів і не тільки. Для початку роботи із сервісом, необхідно нажати відповідну кнопку, як на рисунку 3.5.6.

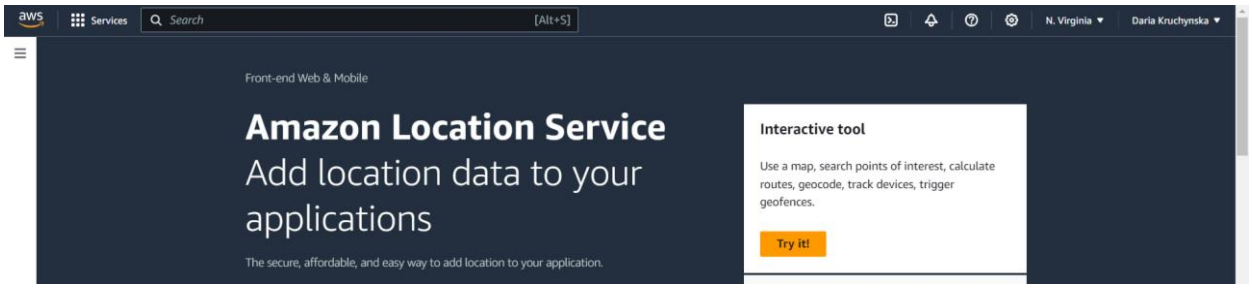

Рисунок 3.5.6 – Початок налаштування сервіса Amazon Location Service

Далі обираємо провайдера послуги, як на рисунку 3.5.7. Використання сервісу є також платним, але перші три місяці безкоштовні, тому на перший час цього достатньо, а далі кошти будуть зніматись відповідно до налаштувань та використання.

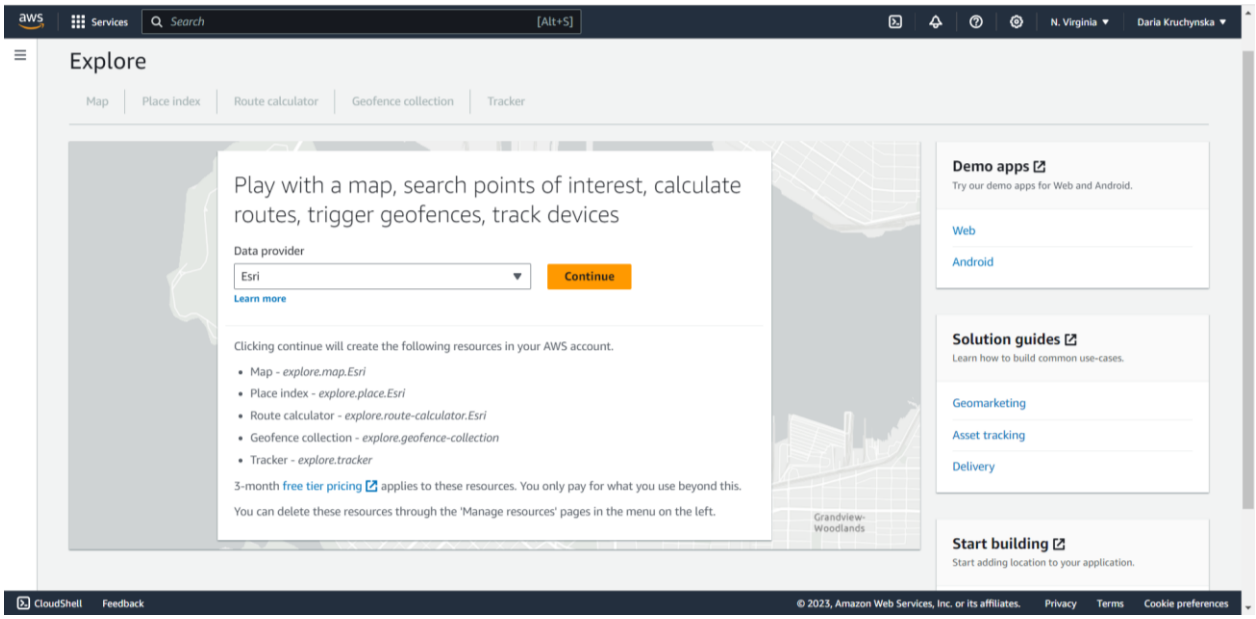

Рисунок 3.5.7 – Обрання провайдера для надання послуг

Після обрання провайдера, налаштовуються координати місцезнаходження, як на рисунку 3.5.8.

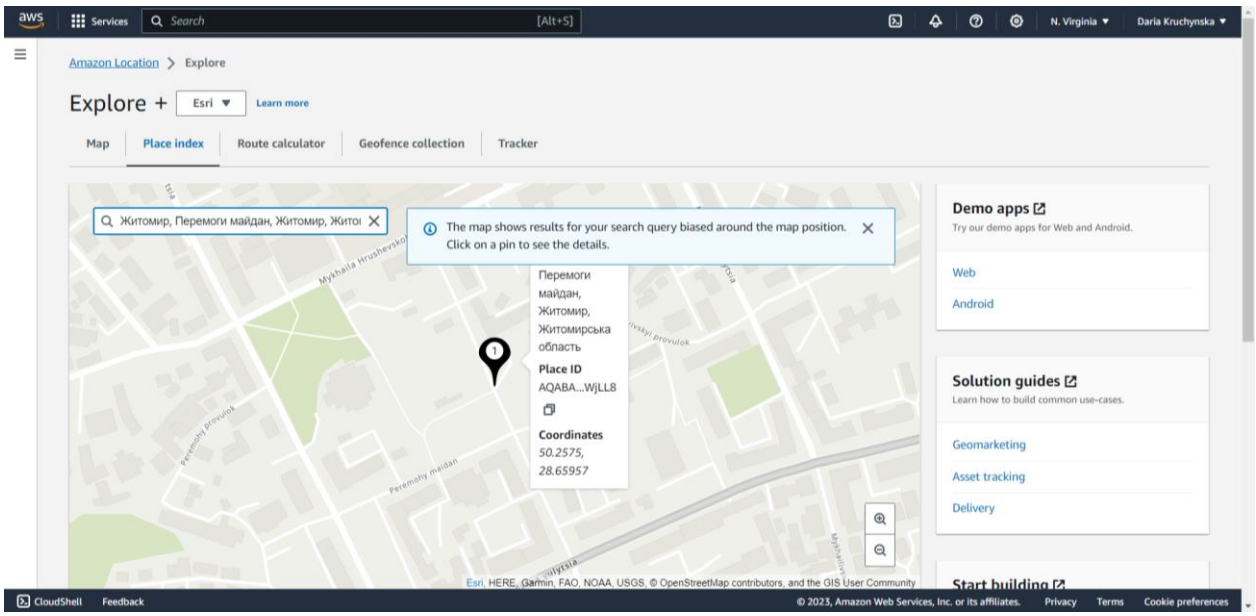

Рисунок 3.5.8 – Налаштування координат місцезнаходження

Після цього формується запит API та відповідь. Даний запит API можна буде використовувати у майбутньому програмному коді додатка, для реалізації як прикладу функціонування. Або ж можна буде згенерувати новий API запит та відповідь, відповідно до місцезнаходження інтернет-магазину, якщо локація зміниться у майбутньому. Після всіх налаштувань в результаті створюється індекс місця, як на рисунку 3.5.9.

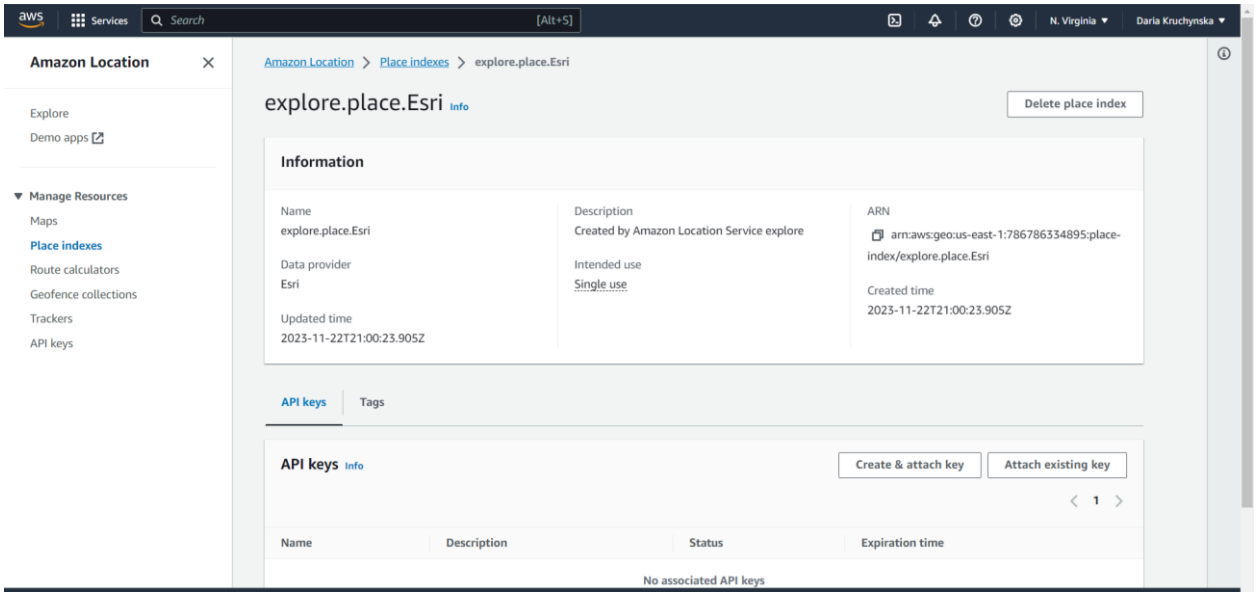

Рисунок 3.5.9 – Успішно створений індекс місцезнаходження

Для даного етапу сервісів для комерційної частини достатньо. В майбутній розробці, звичайно при потребі можна буде розгорнути ще декілька сервісів.

Висновки до розділу 3

У третьому розділі реалізовувалась архітектура хмарної інфраструктури на практиці, яка розроблялась у попередньому розділі, тобто другому. Під час реалізації було обґрунтоване використання тих сервісів, які підходять для функціонала.

Третій розділ вмістив у себе реалізацію різних частин інфраструктури, найголовнішими були клієнтська та серверна, так як вони лягають в основу подальшої розробки. Також важливими частинами являється захист системи та авторизація користувачів з методами доступу до веб-додатка, що в свою чергу також реалізовує додатковий захист. Був проведений аналіз доцільності використання сервісів на даний час розробки та на перспективу розробки в залежності від бюджету проєкту. Невід’ємною частиною інтернет-магазину є комерційна складова, яка реалізувалась під ті потреби, які є актуальними на сьогодні, тобто пошукова система та сервіс місцезнаходження.

ВИСНОВКИ

Використання хмарних інфраструктур для різних сфер бізнесу відкриває нові можливості та допомагає залишатися на високому рівні у такий швидкий час диджиталізації суспільства. Адже зберігати інформацію та керувати нею в будь-який час, робить тебе мобільним та конкурентоспроможним, не в залежності від того, чи ти клієнт бізнесу який у хмарі, чи власник бізнесу який здійснив міграцію у хмару.

Найголовніше, що такі можливості доступні не лише для сфер бізнесу, а й для інших корпорацій чи установ державного сектору, або ж банківського тощо. При реалізації хмарної інфраструктури, хмарні провайдери зі своєї сторони надають високий рівень зручного керування та найголовніше інформаційної безпеки. При цьому всьому є можливість у використанні різного типу інструментів, для аналізування, обробки і т.д., конфіденційної інформації, для отримання результатів, що покращить роботу в подальшому.

Хмарна інфраструктура – це система хмарних обчислень, яка включає в себе компоненти та технології, такі як апаратні засоби, сховища даних, мережеві та абстрактні ресурси тощо, у довільному вигляді в залежності від потреб компанії.

Саме для інтернет – магазину, особливо якщо цей магазин має велику базу клієнтів, або ж він є гуртовий, відповідно в такому магазині широкий спектр товарів на вибір, тому для рішення низки питань обирають хмарну інфраструктуру. Інтернет – магазини кожного дня відвідує велика кількість людей, яка може сягати десятків тисяч, тому необхідні потужності, які будуть мати змогу витримувати різні види навантажень.

Під час виконання кваліфікаційної роботи було виконано дослідження актуальності теми проєкту захищеної архітектури хмарної інфраструктури для інтернет-магазину, побудованої на базі AWS. В ході виконання було визначено мету, об’єкт та предмет дослідження.

В процесі виконання дослідження проаналізовано існуючі поняття «хмарні технології», що дало змогу визначити оптимальний варіант та

актуальність використання хмарних технологій в загальному. Огляд сучасних хмарних технологій, а саме: їх типів, моделей, принципів застосування у різних сферах роботи, надало можливість визначити переваги та недоліки в загальному вигляді та уточнити на деяких моментах, чи можливо їх уникнути в майбутньому.

Створений акаунт у системі AWS надав можливість більш детально оглянути всі існуючи сервіси та зробити висновок для визначення найактуальніших категорій даних сервісів та їх підкатегорій. Був проведений не тільки аналіз самих сервісів, а розглянуто їх принципи роботи. Особлива увага приділена саме сервісам захисту.

Детальний аналіз сервісів надав можливість розробити доцільну архітектуру для хмарної інфраструктури інтернет-магазину, враховуючи навіть нюанси бюджету. Дана архітектура являється каркасом інфраструктури, що дало можливість реалізувати її на практиці.

А саме виходячи з попередніх досліджень, аналізу та створеної архітектури, було розгорнуто сервіс для аутентифікації клієнтів Amazon Cognito та зареєстроване доменне ім’я dsluxury.net використовуючи сервіс Amazon Route 53.

Після чого було розгорнуто клієнтську частину та серверну хмарної інфраструктури, які включали в себе такі сервіси: AWS Fargate, Amazon ElastiCache та AmazonDynamoDB. Додатково у серверній частині було реалізовано сервіс AWS Lambda та взаємодію між даними частинами використовуючи Amazon API Gateway.

Важливою частиною хмарної інфраструктури стала безпека, у якій був розгорнутий сервіс AWS WAF. Було розгорнуто сервіси для забезпечення хмарної інфраструктури, а саме для пошуку місцезнаходження Amazon Location Service та пошукову систему Amazon OpenSearch Service.

В результаті створена хмарна інфраструктура, яка була реалізована на базі AWS. Дана хмарна інфраструктура є захищеною та більш автоматизованою, та спрощеною, як для співробітників майбутнього інтернет – магазину, так і

для користувачів. Важливим моментом є те, що спроєктована захищена хмарна інфраструктура є універсальною, та легко адаптується під різні сфери майбутнього інтернет-магазину, будь-то магазин косметики чи спорт товарів.

Все ж таки міграція у хмару, на сьогодні ще залишається одним з головних рішень для цифрового розвитку компанії, установи чи банку. Незважаючи на всі переваги та перспективи, рішення переходу у хмару не є вирішенням усіх питань та проблем. Дане рішення не знімає відповідальність з компанії у регулярному пошуку для вдосконалення свого бізнесу саме з цифрового боку. Будь-яка компанія, яка обирає хмарні технології для свого бізнесу, повинна не полишати пошук та застосування передових методів керування інформацією. Необхідність оцінки та винайдення рішень для мінімізації будь-яких ризиків, яка є притаманною для класичної IT-інфраструктури залишається і для хмарної. Але звичайно, що з часом це може змінитись.

Підбиваючи підсумки, варто зазначити, що міграція у хмару та створення хмарної інфраструктури, підвищує ефективність роботи, що в результаті використання дає змогу зменшити витрати на експлуатацію, керування та масштабованість. Перехід у хмару не є легким шляхом, такий вибір потребує ретельного планування, так, як відбуваються зміни у подальшій роботі та експлуатації такої системи. Але всі зусилля, які докладаються для цифровізації бізнесу, вже найближчим часом показують результати.

Випливаючи з вище зазначеного, можна зробити висновок, що мета кваліфікаційної роботи успішно реалізована та досягнута.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cloud Security Alliance’s Security Guidance for Critical Areas of Focus in Cloud Computing v4.0/CSA. – 2021.- Режим доступу до ресурсу: https://cloudsecurityalliance.org/download/securityguidance-v4/

2. Про хмарні послуги: Закон України від 17.02.2022 № 2075-IX. – Режим доступу до ресурсу: https://ips.ligazakon.net/document/view/t222075?an=1&ed=2022_02_17

3. Про використання банками хмарних послуг в умовах воєнного стану в Україні: Постанова Правління Національного банку України від 08.03.2022 № 42. – Режим доступу до ресурсу: https://bank.gov.ua/ua/legislation/Resolution_08032022_42

4. Інформаційне забезпечення юридичної діяльності: підручник / кол. авт.; ред. В.Б. Вишня. – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. – 245 с.

5. NIST (National Institute Of Standards And Technology). 1995. An Introduction to Computer Security: The NIST Handbook. (Special Publication 800-145).

6. Андрощук, О., Головченко, О., Литовченко, Г. і Петрушен, М. (2021) «Аналіз поняття хмарні технології: види, категорії, переваги та недоліки», Молодий вчений, 6 (94), с. 83-87.

7. Таранова Є. Міграція в “хмару”: чому у воєнний час хмарні технології допоможуть убезпечити бізнес – 2022. – [Електронний ресурс]. – Режим доступу: https://delo.ua/uk/telecom/migraciya-v-xmaru-comu-u-vojennii-cas-xmarni-texnologiyi-dopomozut-ubezpeciti-biznes-397106/

8. Хмарно і фізично в Україні. Чому міграція до локального дата-центру вже на часі. – Датацентр «Парковий». – 2023. – [Електронний ресурс]. – Режим доступу: https://ain.ua/2023/07/25/hmarno-i-fizychno-v-ukrayini-chomu-migracziya-do-lokalnogo-data-czentru-vzhe-na-chasi-dataczentr-parkovyj/

9. Найкращі хмарні сервіси України у 2022 році: дослідження Molfar – 2022. – [Електронний ресурс]. – Режим доступу:

https://ain.ua/2022/09/15/najkrashhi-hmarni-servisy-ukrayiny-u-2022-roczi-doslidzhennya-molfar/

10. Вакалюк Т. А. Огляд існуючих моделей хмарних послуг для використання у вищих навчальних закладах. Тези доповідей VIII Міжнародної науковотехнічної конференції "Інформаційно-комп'ютерні технології – 2016" (22– 23 квітня 2016 р.). Житомир: ЖДТУ, 2016. С. 215-217.

11. Кожному своя «хмара» — якими бувають cloud-сервіси та яка між ними різниця — Na chashi. – 2017. [Електронний ресурс]. – Режим доступу: https://nachasi.com/2017/10/02/cloudservis/

12. Хмарні обчислення: приклади використання та переваги — On your Business. – 2021. – [Електронний ресурс]. – Режим доступу: https://onbiz.biz/cloud-usage-examples/

13. Навіщо бізнесу «хмари»? Застосування хмарних технологій та їх переваги для бізнесу – SIM Networks. – 2021. – [Електронний ресурс]. – Режим доступу: https://www.sim-networks.com/ukr/blog/clouds-for-business

14. Навіщо вашому бізнесу хмари? 5 сценаріїв використання – Business Special. – 2023. – [Електронний ресурс]. – Режим доступу: https://ain.business/2023/04/26/navishho-vashomu-biznesu-vykorystovuvaty-hmary-5-sczenariyiv-vykorystannya/

15. Савицька Н. Л. Маркетинговий цикл Customer Development в умовах цифровізації // Інноваційні технології маркетингу і менеджменту в умовах трансформаційних змін : тези доп. Міжнар. наук.-практ. конф. (27–29 квітня 2023 р., м. Хмельницький). – Хмельницький : ХНУ, 2023. – 203 с

16. Биков В.Ю. Теоретико-методологічні засади формування хмаро орієнтованого середовища вищого навчального закладу / В.Ю. Биков, М.П.Шишкіна // Теорія і практика управління соціальними системами. –2016. –No2. –С. 30-52.

17. Хмарні технології для сфери охорони здоров'я. – [Електронний ресурс]. – Режим доступу: https://gigacloud.ua/services/hmarni-tehnologii-dlja-mediciny

18. 5 Medtech-трендів для сфери охорони здоров’я у 2023 – Київстра Бізнес. – 2023. – [Електронний ресурс]. – Режим доступу: https://hub.kyivstar.ua/news/5-medtech-trendiv-dlya-sfery-ohorony-zdorov-ya-u-2023/

19. Сідлецька Д. Проблеми безпеки в хмарі/ Сучасні комп’ютерні системи та мережі в управлінні: V Всеукр. науково-прак. інтер- конф. студ., асп. та мол. вч., 30 лист. 2022 р. – Хмельницький, 2022.

20. Сідлецька Д. Перспективи використання динамічних протоколів керування Vlan – мережами у хмарних сервісах/ Сучасні комп’ютерні та інформаційні системи і технології: III Всеукр. науково-прак. Інтер- конф., Запоріжжя, 12 – 19 груд. 2022 р. – Запоріжжя, 2022.

21. Мелло Д. «11 найпопулярніших хмарних загроз безпеки» [John P. Mello Jr. 11 top cloud security threats.] ЦСО Онлайн [CSO Online]/ Джон Мелло. – 2022. – Режим доступу до ресурсу: https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

22. Амазон Веб Сервіс: науковий центр [Amazon Web Servises: Knowledge Center] – [Електронний ресурс]. – Режим доступу: https://repost.aws/knowledge-center.

23. Хмарні конкурентні вектори, експлойти та загрози (CAVEaT™): нова матриця загроз для співпраці в галузі [Cloud Adversarial Vectors, Exploits, and Threats (CAVEaT™): An Emerging Threat Matrix for Industry Collaboration]/ [Cloud Security Alliance] CSA. – 2023.- Режим доступу до ресурсу: https://cloudsecurityalliance.org/artifacts/cloud-adversarial-vectors-exploits-and-threats/

24. Основні загрози для хмарних обчислень: пандемія 11. Глибоке занурення [Top Threats to Cloud Computing: Pandemic 11 Deep Dive]/ [Cloud Security Alliance] CSA. – 2023.- Режим доступу до ресурсу: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven-deep-dive/

25. Як створити безпечну безсерверну архітектуру [How to Design a Secure Serverless Architecture]/ [Cloud Security Alliance]CSA. – 2023.- Режим доступу до ресурсу: https://cloudsecurityalliance.org/artifacts/how-to-design-a-secure-serverless-architecture/

26. «Основні загрози Cloud Security Alliance для хмарних обчислень: Звіт про пандемію 11 показує, що традиційні проблеми безпеки хмарних технологій стають менш занепокоєними» [Cloud Security Alliance's Top Threats to Cloud Computing: Pandemic 11 Report Finds Traditional Cloud Security Issues Becoming Less Concerning] Офіційний пресреліз CSA [Cloud Security Alliance(CSA) Official Press Release]/CSA. – 2022. – Режим доступу до ресурсу: https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/