

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний технічний університет «Дніпровська політехніка»



## ЗВІТ

з лабораторної роботи №4

з дисципліни «Аналіз програмного забезпечення»

*Виконав:*

ст.гр. 122-21-1

Шевченко Іван Богданович

*Перевірів(-ла):*

асистент Шевченко Ю.О.

м. Дніпро

2024 рік

**Завдання:** Зареєструватись в системі AWS (Amazon web services). Дали розмістити на сервісі S3 статичну веб сторінку на якій буде вказана ваше ПІБ та обов'язково академічна група. Бакет на S3 в якому буде лежати ваша сторінка обов'язково в своєму імені повинен містити ваше прізвище та ім'я. Наприклад `myefremov-bucket-apz` для студента з іменем Михайло Єфремов. Результатом виконання цієї лабораторної роботи буде адреса на вашу веб-сторінку на подібні `myefremov-bucket-apz.amazonaws.com/index.html` на якій буде написано ваш ПІБ та група.

## Практична частина:

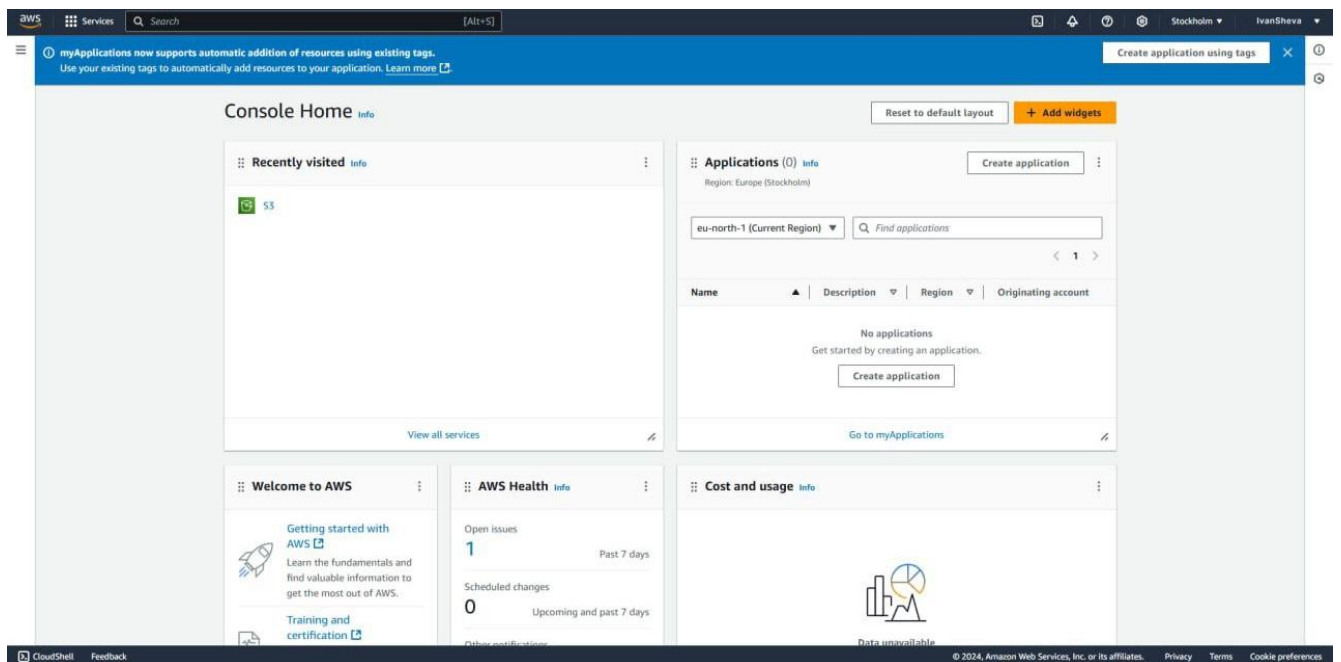
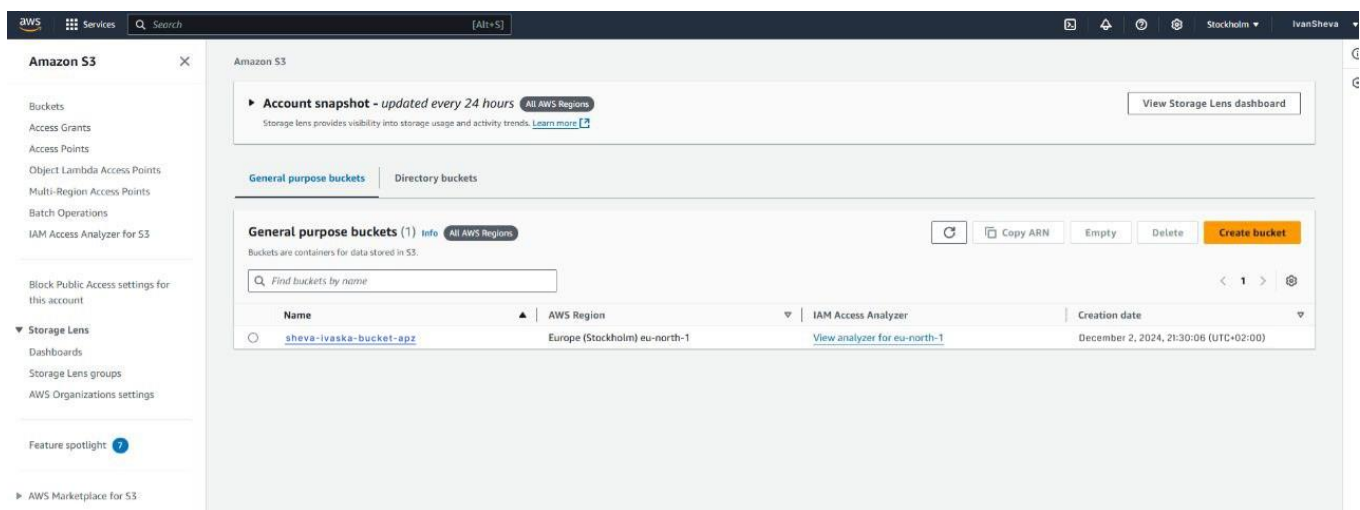


Рис.1 – виконано реєстрацію на сайті AWS (усі карткові перевірки успішно пройдено)



Services
Search
[Alt+S]

Amazon S3
> Buckets
> Create bucket

## Create bucket Info

Buckets are containers for data stored in S3.

### General configuration

AWS Region  
Europe (Stockholm) eu-north-1

Bucket type Info

☒ **General purpose**  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info

myawsbucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*  
Only the bucket settings in the following configuration are copied.

**Choose bucket**

Format: s3://bucket/prefix

### Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.


Рис.2, 3 – авторизовано у сервісі Amazon S3 і створено особисте відерце загального призначення (general purpose bucket), у якому вказано налаштування для створення статичної сторінки

### Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.


**Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

### Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable
 ☐ Enable

### Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Add tag

### Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)
 ☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable
 ☒ Enable

### Edit bucket policy Info

#### Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Policy examples [Policy generator](#)

Bucket ARN

arn:aws:s3:::sheva-ivaska-bucket-apz

#### Policy

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": "s3:GetObject",
9       "Resource": "arn:aws:s3:::sheva-ivaska-bucket-apz/*"
10    }
11  ]
12 }
```

#### Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

Рис. 4, 5, 6 – надання bucket policy параметрів, які дозволять сайту відкриватися ззовні (деблокування public access і ефект allow для publicreadgetobject)

## Результат:

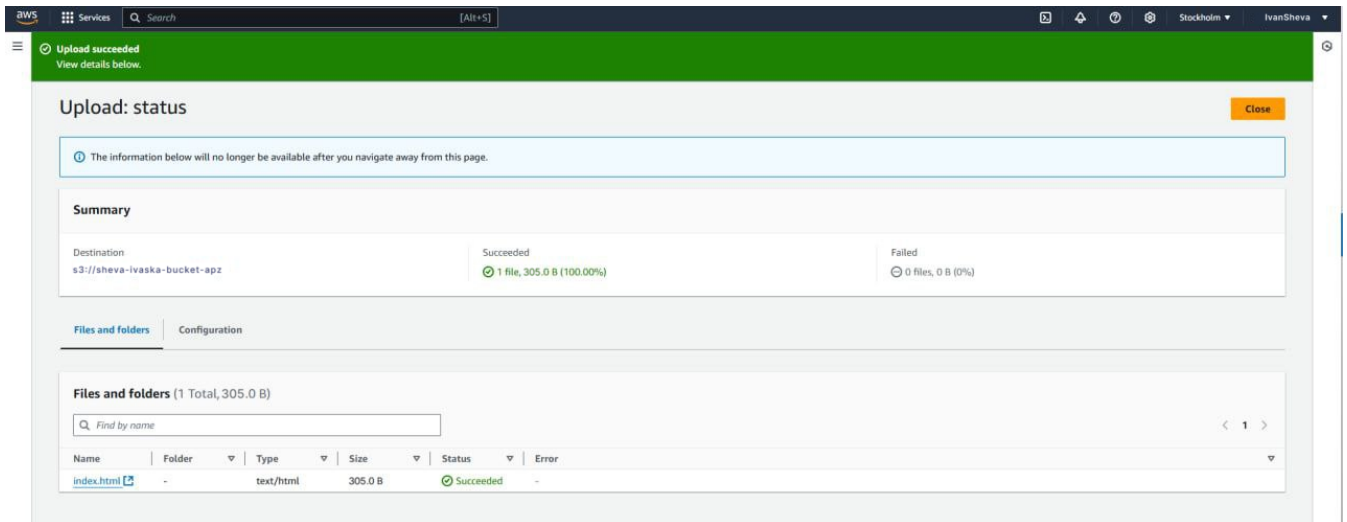


Рис. 7 – завантаження файлу index.html у особистий bucket пройшло успішно



Рис.8 – URL-посилання на веб-сторінку файлу index.html

# Шевченко Іван Богданович

Група 122-21-1

Рис.9 – відображення змісту index.html на веб-сторінці

**Висновок:** під час виконання лабораторної роботи проведено ознайомлення з принципами роботи системи AWS, покроково досліджено алгоритм розміщення на її сервісі S3 статичної веб-сторінки шляхом створення бакету і встановлення його параметрів.