

Міністерство освіти і науки України
Національний технічний університет «Дніпровська політехніка»



ЗВІТ
про виконання лабораторної роботи №4
з дисципліни
«Аналіз програмного забезпечення»

Виконали студенти: гр. 121-22-3
Антіпов Руслан Миколайович

Прийняв: Шевченко Ю. О.

Дніпро
2025

Тема: AWS S3.

Мета: Набування навичок у створення і розміщенні статичної веб-сторінки на AWS S3.

Основні кроки виконання:

Крок 1. Зареєструватися в системі AWS.

Крок 2. Створити бакет у S3 з вашим прізвищем та іменем.

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](#)

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn more](#) [↗](#)
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

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.
Object Ownership
☒ **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.
Object Ownership
Bucket owner enforced

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.

Крок 3. Розмістити на S3 статичну веб-сторінку, яка містить ваше ПІБ та Вашу академічну групу.

```
index1.html > html
1  <!DOCTYPE html>
2  <html lang="uk">
3  <head>
4    <meta charset="UTF-8">
5    <title>Моя сторінка</title>
6  </head>
7  <body>
8    <h1>Антіпов Руслан Миколайович</h1><br />
9    <p>121-22-3</p>
10 </body>
11 </html>
```

Крок 4. Налаштування хостингу і отримання публічної адреси сторінки, наприклад:

<https://kbaleiko-bucket-apz.s3-website.eu-north-1.amazonaws.com/>

Edit static website hosting [Info](#)

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

- ☐ Disable
☒ Enable

Hosting type

- ☒ Host a static website
Use the bucket endpoint as the web address. [Learn more](#)

- ☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

ⓘ For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

1

JSON Ln 1, Col 1 Errors: 0 Warnings: 0

Cancel

Save changes

мій приклад для перевірки:

<http://rantipov-bucket-apz.s3-website.eu-north-1.amazonaws.com>

