

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»



ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра системного аналізу та управління

Індивідуальне завдання 4

з дисципліни

«Аналіз програмного забезпечення»

Виконав: студент групи 121-22-2

Приходько Кирило Юрійович

Перевірив:

ас. кафедри САУ Шевченко Ю. О

Дніпро 2025

<http://prykhodko121-22-2.com.s3-website.eu-north-1.amazonaws.com/>

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 (the most common)
 Standard - objects are stored in multiple availability zones.
 Directory - objects are stored in one location. They take up very little storage cost due to 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, A-Z, periods (.), and hyphens (-). [Learn more](#)

Copy settings from existing bucket - optional
Select a bucket whose settings you want to copy.

[Choose bucket](#) [Paste URL](#) [Get started](#)

Object Ownership [info](#)
Controls who can write 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 the bucket are owned by the account. Access to the bucket and its objects is controlled by individual object ACLs.

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

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 to the bucket and all objects within it. If you are using a bucket policy or any other type of policy, 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 case. [Learn more](#)

Block all public access
 Block public access to buckets and objects granted through new access control lists (ACL)
 Block public access to buckets and objects granted through new bucket or access point policies
 Block public access to buckets and objects granted through any access control lists (ACL)
 Block public access to buckets and objects granted through new public bucket or access point policies
 Block public and private access to buckets and objects through any public bucket or access point policies
Or set specific public and private access rules for buckets or objects with policies that grant public access to buckets and objects.

Turning off 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

© 2021, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)