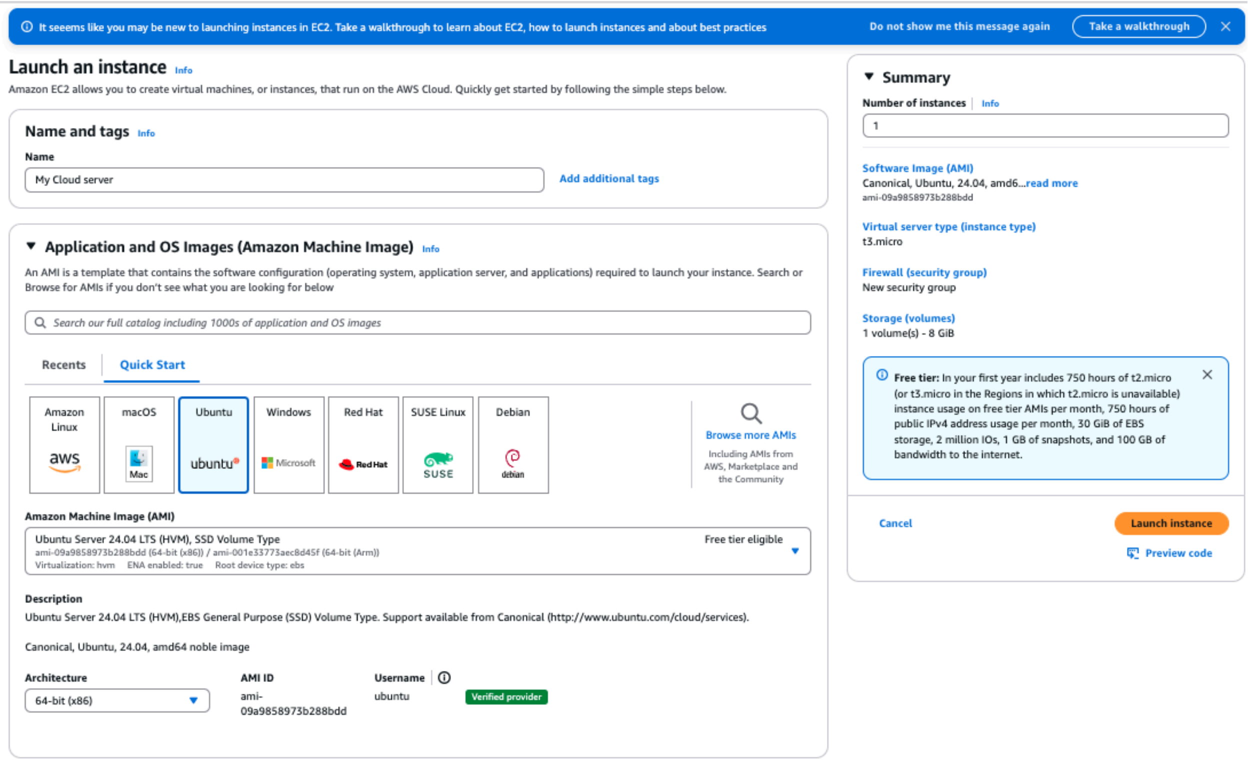
Grand Assignment Cloud Computing SYED MURTAZA HASSAN DS221026

1. Create an EC2 Instance

Step 1: Name your EC2 Instance and select your desired Application OS Image and architecture.



It seeems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices — Do not show me this message again — Take a walkthrough

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: My Cloud server — Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Linux | Debian

Browse more AMIs — Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-09a9858973b288bdd (64-bit (x86)) / ami-001e33773aec8d45f (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture: 64-bit (x86)
AMI ID: ami-09a9858973b288bdd
Username: ubuntu — Verified provider

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04, amd6...read more
ami-09a9858973b288bdd

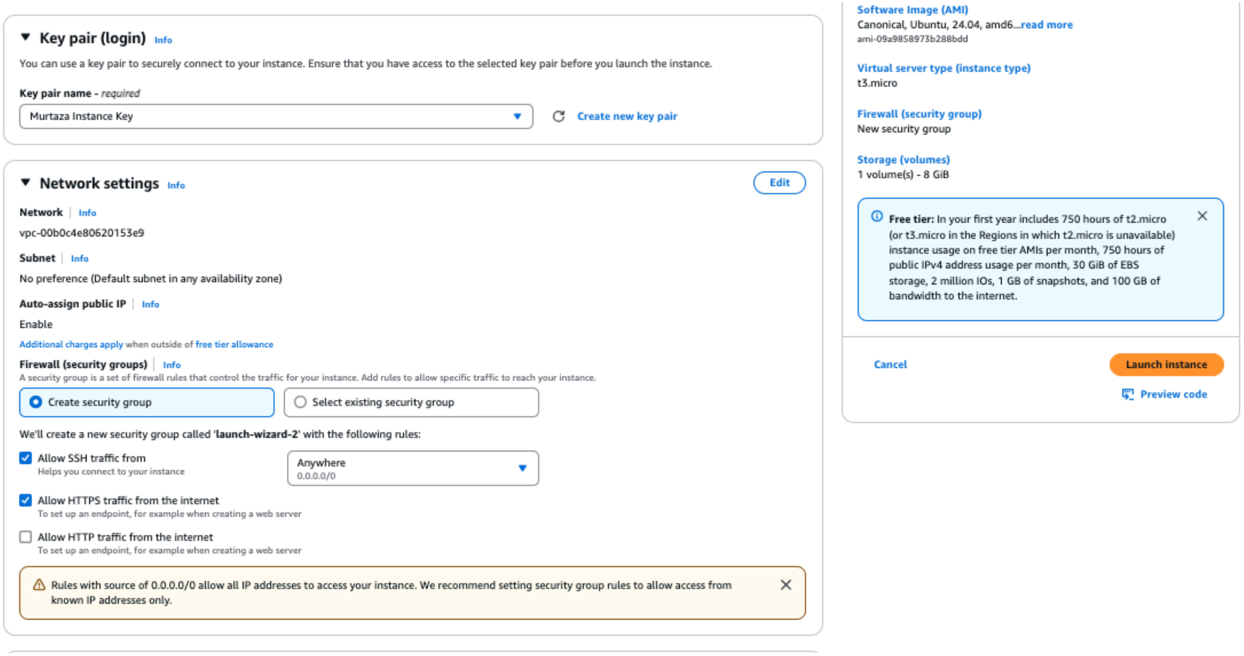
Virtual server type (instance type): t3.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Step 2: Now generate a key pair and save it locally on your PC and allow traffic from SSH and Known IP Addresses.



Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: Murtaza Instance Key — Create new key pair

Network settings Info — Edit

Network: vpc-00b0c4e80620153e9

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

☑ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Software Image (AMI): Canonical, Ubuntu, 24.04, amd6...read more
ami-09a9858973b288bdd

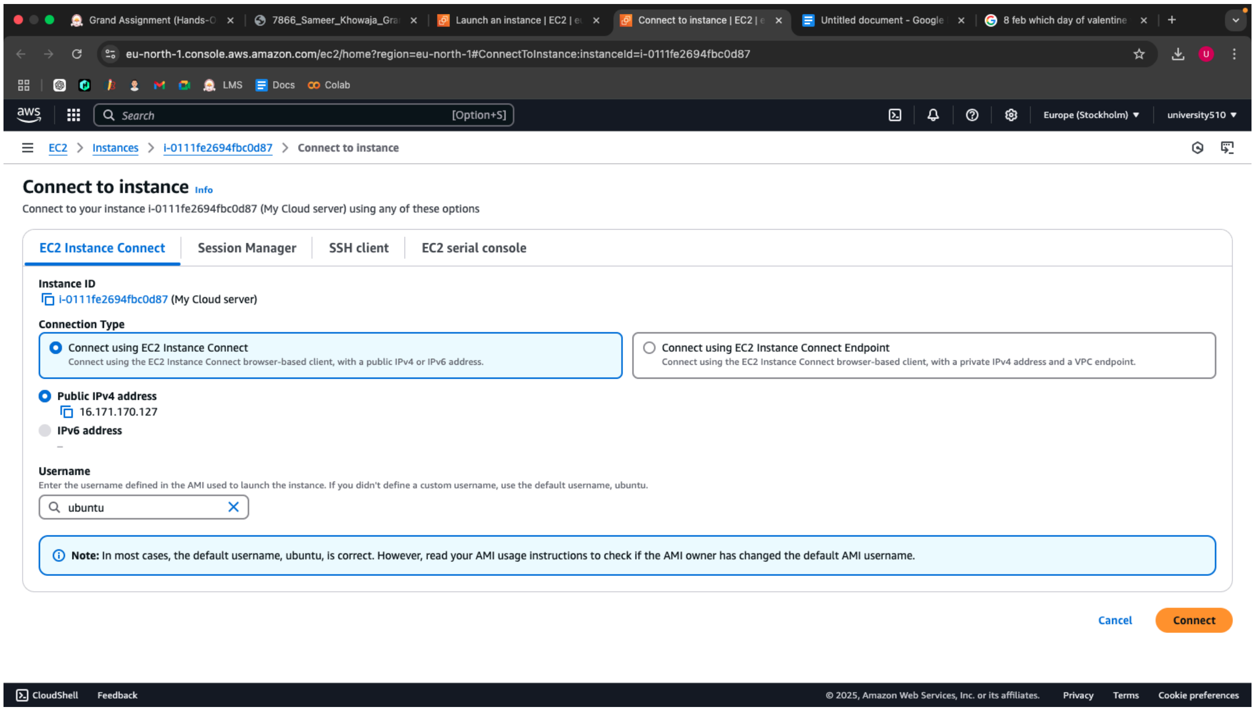
Virtual server type (instance type): t3.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Remaining all the settings during the instance creation will remain the same. Step 3: Once created, start the EC2 instance and choose your connection type:


Grand Assignment (Hands-O
7866_Sameer_Khowaja_Gra
Launch an instance | EC2 | eu
Connect to instance | EC2 | e
Untitled document - Google
8 feb which day of valentine
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#ConnectToInstance:instanceId=i-0111fe2694fbc0d87
LMS
Docs
Colab
aws
Search
[Option+S]
Europe (Stockholm) ▼
university510 ▼
EC2 > Instances > i-0111fe2694fbc0d87 > Connect to instance

Connect to instance Info

Connect to your instance i-0111fe2694fbc0d87 (My Cloud server) using any of these options

EC2 Instance Connect
Session Manager
SSH client
EC2 serial console

Instance ID
i-0111fe2694fbc0d87 (My Cloud server)

Connection Type

● Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 or IPv6 address.

○ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

● Public IPv4 address
16.171.170.127

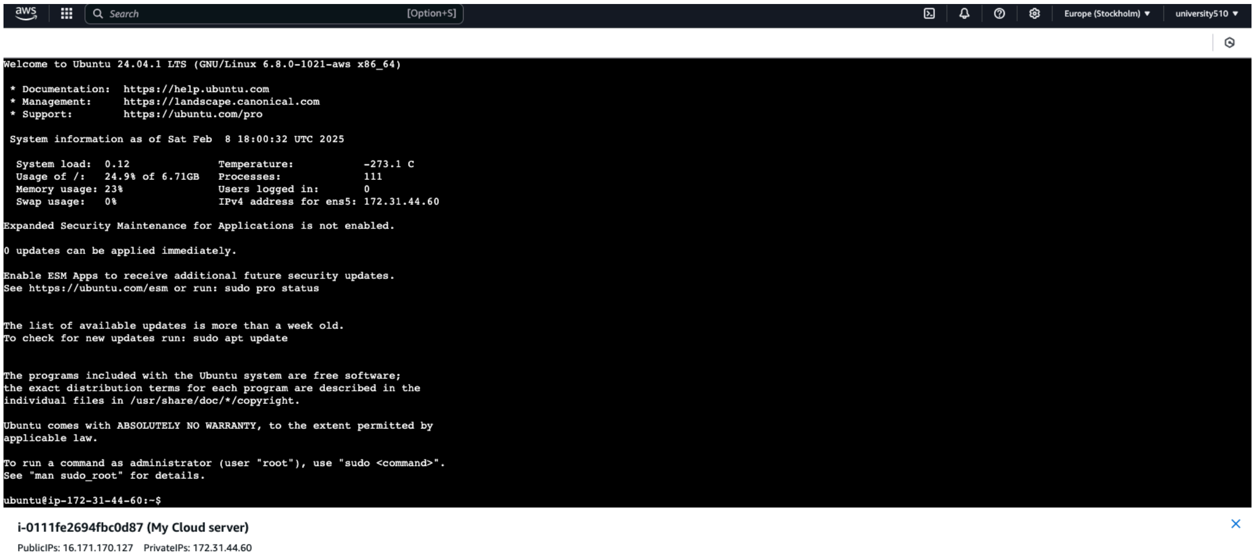
○ IPv6 address
–

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ubuntu.

ubuntu

Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Step 4: After following these steps, our connection with cloud will be established and now you can easily perform activities.

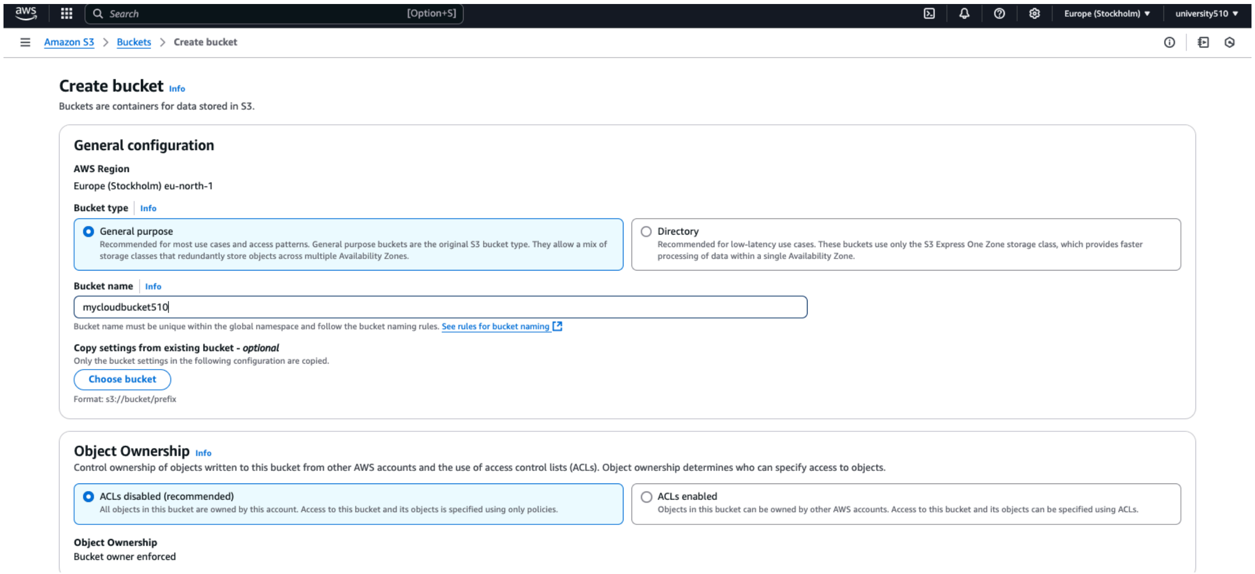


```
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1021-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sat Feb  8 18:00:32 UTC 2025

  System load:  0.12               Temperature:           -273.1 C
  Usage of /:   24.9% of 6.71GB    Processes:             111
  Memory usage: 23%                Users logged in:       0
  Swap usage:   0%                 IPv4 address for ens5: 172.31.44.60

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-44-60:~$
```

i-0111fe2694fbc0d87 (My Cloud server)
PublicIPs: 16.171.170.127   PrivateIPs: 172.31.44.60

Now, as we can see that we are now connected to the EC2 Instance Server.

Create an S3 bucket, upload an image and view it.



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

mycloudbucket510

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

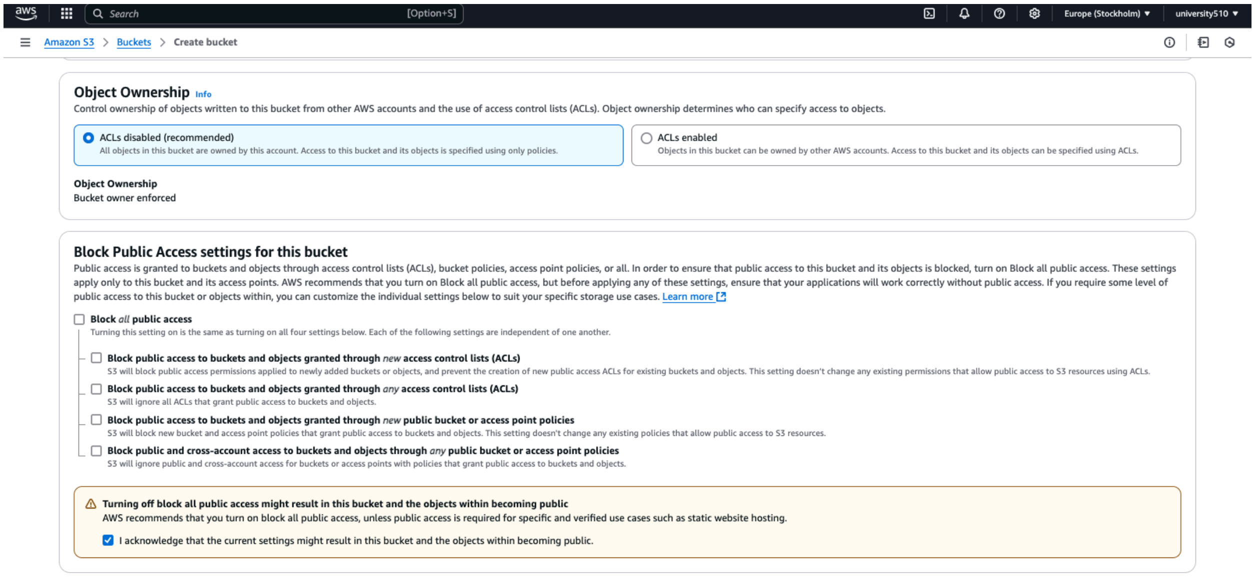
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● 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.

Object Ownership

Bucket owner enforced



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.

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.

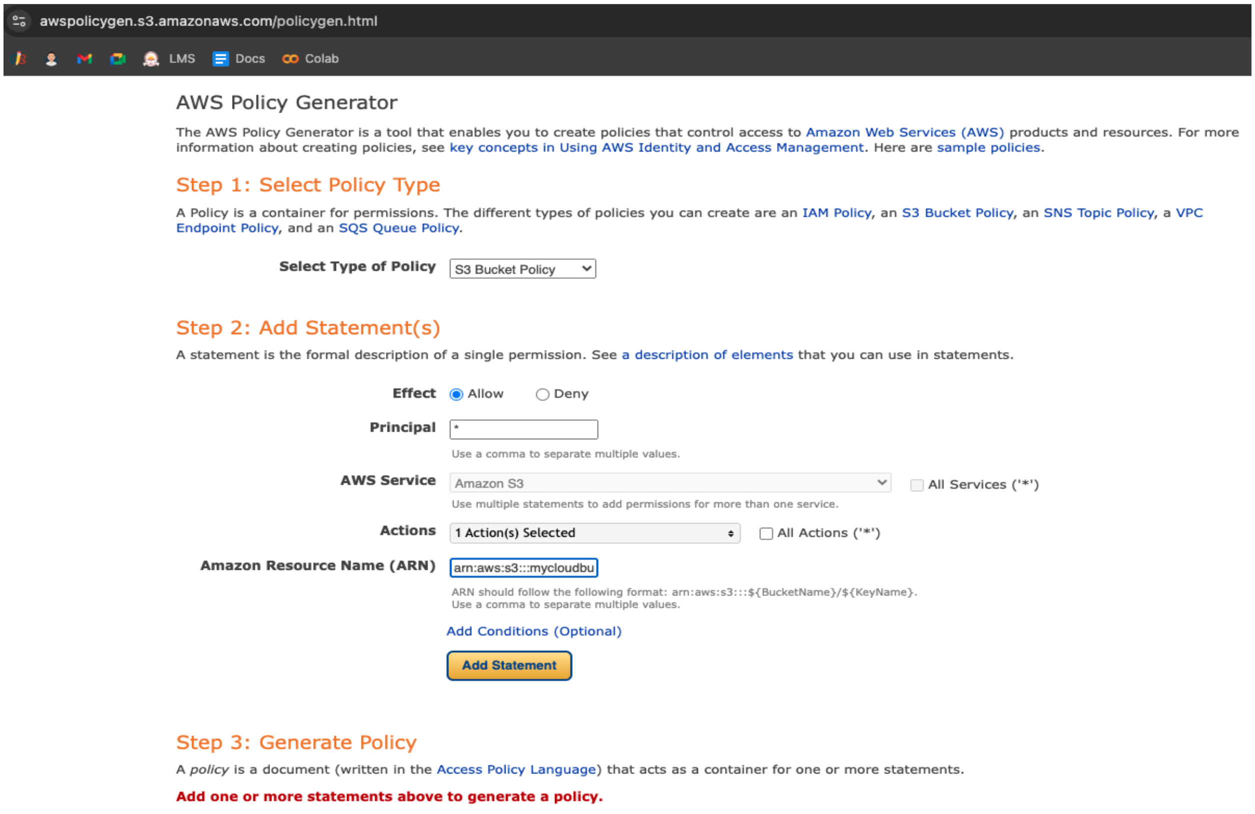
☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Step 2: Once Created, head inside the bucket, move towards the permission and create policy using aws policy generator.
Apply the following policies as

Type of policy: S3 Bucket

Principal: * (ALL)

Actions: Get object ( )



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect ● Allow ○ Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3 □ All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN) arn:aws:s3:::mycloudbu

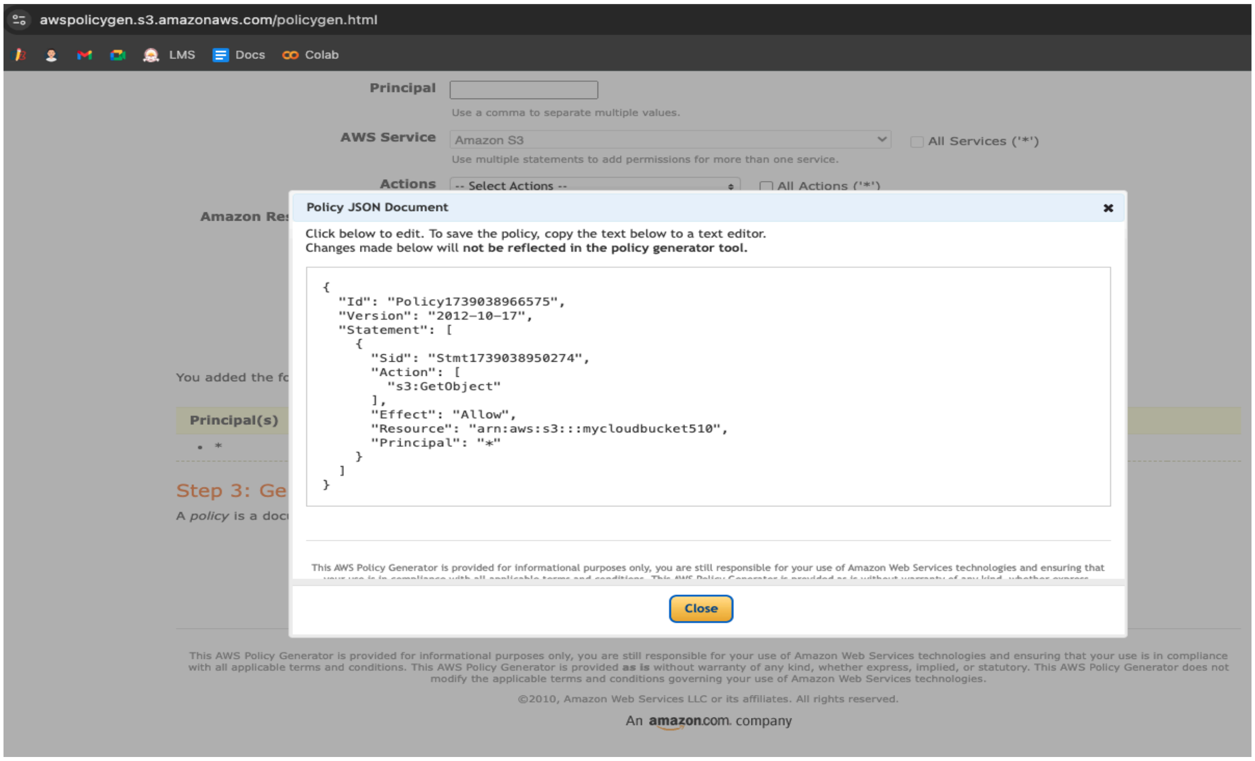
ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.



Principal

Use a comma to separate multiple values.

AWS Service Amazon S3 □ All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- □ All Actions ('*')

Amazon Res

You added the fo

Principal(s)

- *

Step 3: Ge

A *policy* is a docu

Policy JSON Document ×

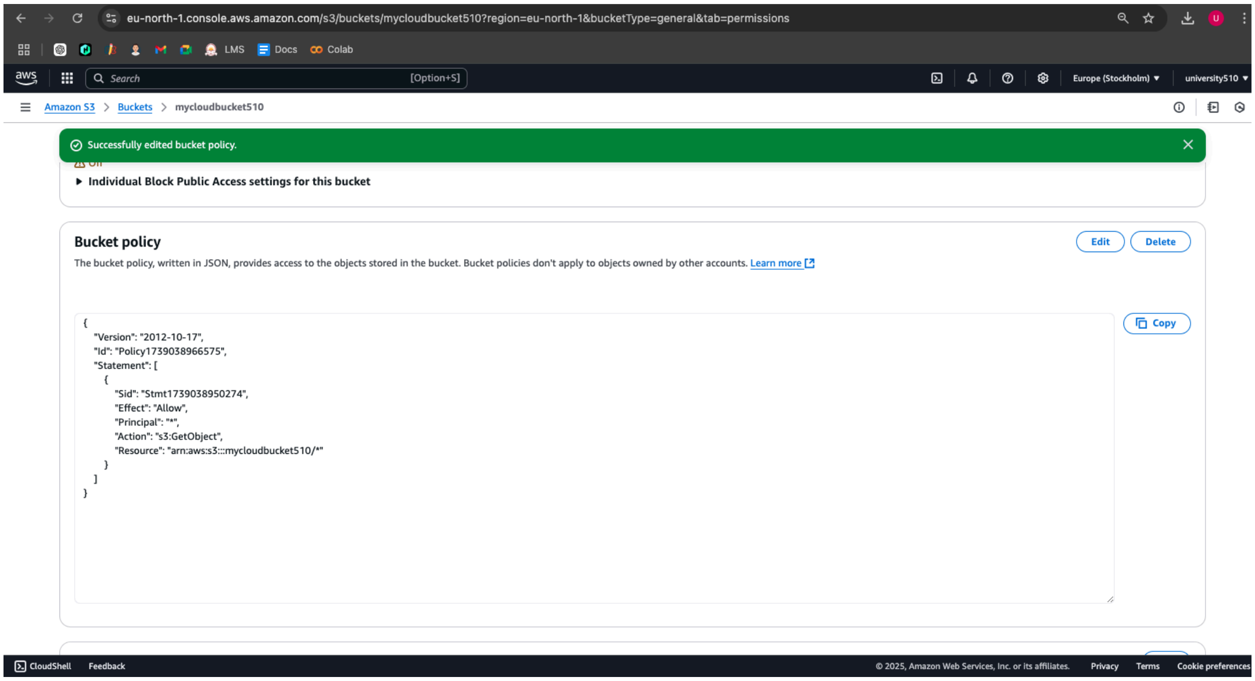
Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Id": "Policy1739038966575",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1739038950274",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mycloudbucket510",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided **as is** without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

An amazon.com. company



eu-north-1.console.aws.amazon.com/s3/buckets/mycloudbucket510?region=eu-north-1&bucketType=general&tab=permissions
LMS
Docs
Colab
aws
Search
[Option+S]
Europe (Stockholm) ▾
university510 ▾
Amazon S3 > Buckets > mycloudbucket510

Successfully edited bucket policy.

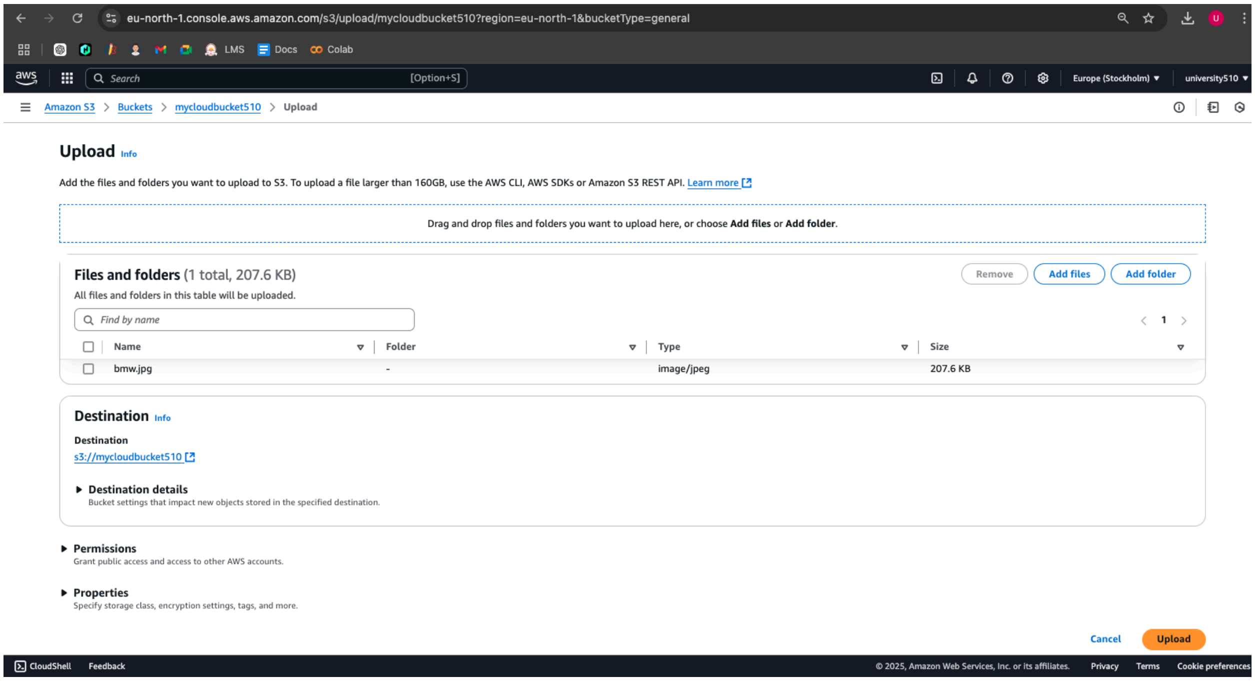
▸ Individual Block Public Access settings for this bucket

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

```
{
    "Version": "2012-10-17",
    "Id": "Policy1739038966575",
    "Statement": [
        {
            "Sid": "Stmt1739038950274",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::mycloudbucket510/*"
        }
    ]
}
```

CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



eu-north-1.console.aws.amazon.com/s3/upload/mycloudbucket510?region=eu-north-1&bucketType=general
LMS
Docs
Colab
aws
Search
[Option+S]
Europe (Stockholm) ▾
university510 ▾
Amazon S3 > Buckets > mycloudbucket510 > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 total, 207.6 KB)

Remove
Add files
Add folder

All files and folders in this table will be uploaded.

□	Name	Folder	Type	Size
□	bmw.jpg	-	image/jpeg	207.6 KB

Destination Info

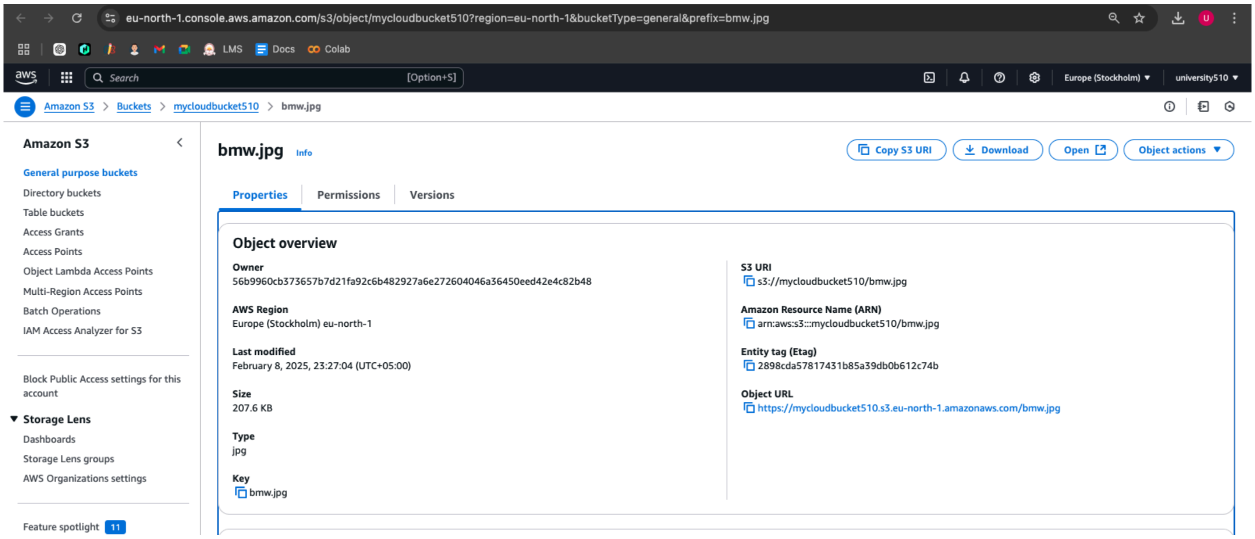
Destination

s3://mycloudbucket510

▸ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

▸ **Permissions**
Grant public access and access to other AWS accounts.

▸ **Properties**
Specify storage class, encryption settings, tags, and more.



eu-north-1.console.aws.amazon.com/s3/object/mycloudbucket510?region=eu-north-1&bucketType=general&prefix=bmw.jpg

bmw.jpg

Object overview

Owner
56b9960cb373657b7d21fa92c6b482927a6e272604046a36450eed42e4c82b48

AWS Region
Europe (Stockholm) eu-north-1

Last modified
February 8, 2025, 23:27:04 (UTC+05:00)

Size
207.6 KB

Type
jpg

Key
bmw.jpg

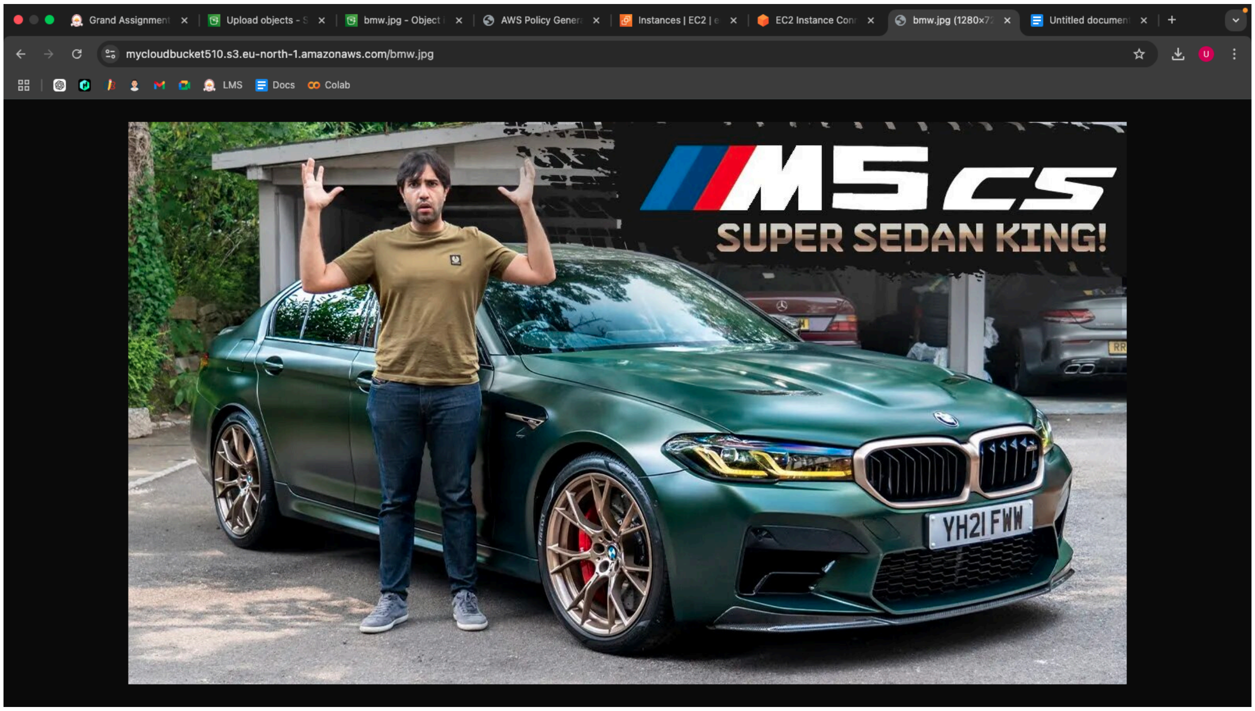
S3 URI
s3://mycloudbucket510/bmw.jpg

Amazon Resource Name (ARN)
arn:aws:s3:::mycloudbucket510/bmw.jpg

Entity tag (Etag)
2898cda57817431b85a39db0b612c74b

Object URL
https://mycloudbucket510.s3.eu-north-1.amazonaws.com/bmw.jpg

https://mycloudbucket510.s3.eu-north-1.amazonaws.com/bmw.jpg



mycloudbucket510.s3.eu-north-1.amazonaws.com/bmw.jpg