

# CLOUD COMPUTING

## GRAND ASSIGNMENT

NAME: Hanzala Rashid

REG# DS221050

### Task #1: Creating EC2 Instance

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

ubuntu

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

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

RecentsQuick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

linux

Debian

debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

▼ Summary

Number of instances Info

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

Cancel

Launch instance

Preview code

Amazon Machine Image (AMI)

CloudShellFeedback

© 2025, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

▼ 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

Hanzala

Create new key pair

▼ Summary

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd6...read more

ami-09a9858973b288bdd

▼ Network settings Info

Edit

Network Info

vpc-0d4d8666dd4e2a207

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

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-5' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere  
0.0.0.0/0

☒ 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

Instances (2) Info

Last updated less than a minute ago

Connect

Instance state ▼

Actions ▼

Launch instances ▼

Find Instance by attribute or tag (case-sensitive)

All states ▼

< 1 >

☐

Name

▼

Instance ID

Instance state

▼

Instance type

▼

Status check

Alarm status

Availability Zone

▼

Public IP

☐

ubuntu

i-015b77acecc56a0f7

Stopped

t3.micro

–

View alarms +

eu-north-1a

–

☐

ds221050

i-07d3b5cf3e09601ba

Stopping

t3.micro

–

View alarms +

eu-north-1b

ec2-13-6

## Task #2: Creating S3 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

hanzalabucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming [2]

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

General purpose buckets (2) Info All AWS Regions

Copy ARN

Empty

Delete

Create bucket

Find buckets by name

< 1 >

☐

hanzalabucket

Europe (Stockholm) eu-north-1

View analyzer for eu-north-1

January 27, 2025, 12:57:22 (UTC+05:00)

☐

hanzalakibalti

Europe (Stockholm) eu-north-1

View analyzer for eu-north-1

February 1, 2025, 15:55:02 (UTC+05:00)

**Blocking all public access, we will create access policy by ourselves and remaining all settings will remain same.**

**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: 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 ()

### 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 -- Select Actions -- ☐ All Actions (\*\*)

Amazon Resource Name (ARN)

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

[Add Conditions \(Optional\)](#)

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::hanzalabucket	None

## Task#4: Updating Bucket Policies

### 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

```
{
  "Version": "2012-10-17",
  "Id": "Policy1737966531565",
  "Statement": [
    {
      "Sid": "Stmnt1737966530670",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::hanzalabucket/*"
    }
  ]
}
```

## Upload JPEG Image in the S3 Bucket

### hanzalabucket

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	FLOWER.jpg	jpg	January 27, 2025, 13:26:10 (UTC+05:00)	8.7 KB	Standard


## Task#5: Showing the picture which was uploaded

Google Keep

hanzalabucket - S3 bucket | S3

FLOWER.jpg (330x220)

hanzalabucket.s3-eu-north-1.amazonaws.com/FLOWER.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=ASI...



Search

4:37 pm 01/02/2025