# Access S3 from a VPC

Gaurav Balpande

**Gaurav Balpande**
NextWork Student



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is the fundamental networking tool which is used for creation of private space within the AWS region. It is needed for security and to easily manage the resources.

## How I used Amazon VPC in this project

In today's project i had learn how to interactwith Amazon S3 which is not in VPC. For this I used tools like EC2 instance,S3 and IAM roles.

## One thing I didn't expect in this project was...

One thing I never expected is that we can even add files with the use of EC2 instance and that too with AWS CLI.

## This project took me...

it took near to 1.30 hr and it slightly easy.

# In the first part of my project...

## Step 1 - Architecture set up

In this step,we are going to build the infrastructure by building one VPC with instance in it. and also some security tool we would apply.

## Step 2 - Connect to my EC2 instance

In this step we are going to launch Ec2 instance and connect to the instance with Amazon instance connect.

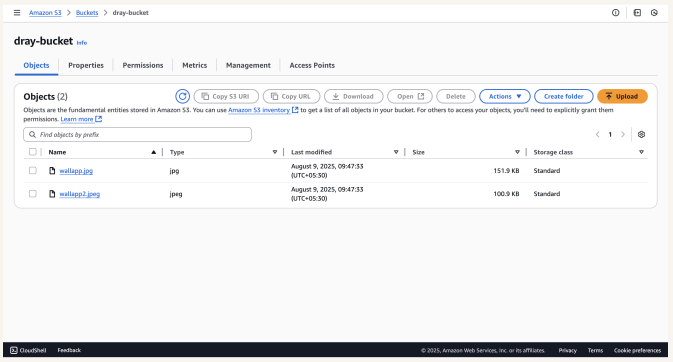
## Step 3 - Set up access keys

In this step,we are going to give the access of AWS resources to the EC2 instance so that it can use various services.

# Architecture set up

I started my project by launching VPC and EC2 instance inide it. I had done this so that later on we can create a connection between EC2 instance S3.

I also set up the AWS S3 by building two files inside a bucket. wallapp.jpg and wallapp2.jpeg



**Gaurav Balpande**
NextWork Student

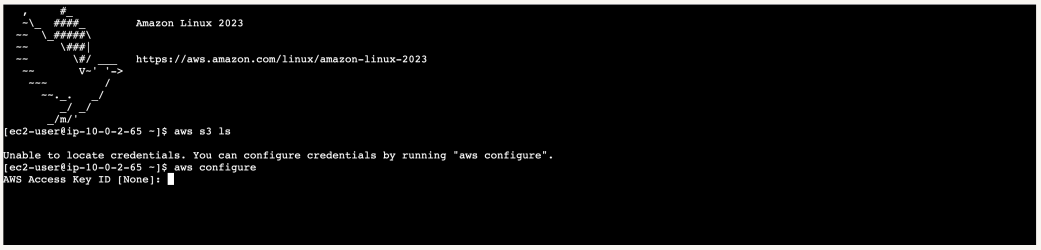


# Running CLI commands

AWS CLI is Amazon command line interface I have access to AWS CLI because with the help of Aws CLI we can access the AWS resources.

The first command I ran was aws s3 ls This command is used to list all the buckets in Amazon S3

The second command I ran was aws configure This command is used to configure the access key and password.



# Access keys

## Credentials

To set up my EC2 instance to interact with my AWS environment, I configured the access key and password this is because Aws cli dont have access on its own to access the AWS resources.

Access keys are like a key with the help of which we get the power to access AWS resources and other things.

Secret access keys are like a password that pair with our access key id.

## Best practice

Although I'm using access keys in this project, a best practice alternative is to use IAM roles. IT gives more security and only give access to definite users.

# In the second part of my project...

## Step 4 - Set up an S3 bucket

In this step,we are going to build two files in one bucket this si because we want to know the list of files in AWS S3 with the help of EC2 instance.

## Step 5 - Connecting to my S3 bucket

In this step,we are heading back to EC2 instance and then will try to run command so that we can the information about Amazon S3.

# Connecting to my S3 bucket

The first command I ran was aws s3 ls This command is used to list all the buckets in Amazon S3

When I ran the command aws s3 ls again, the terminal responded with 2025-08-09 04:16:53 dray-bucket 2025-05-21 19:16:55 elasticbeanstalk-ap-south-1-590183705172 This indicated that we able to access the S3 from the Aws cli.

# Connecting to my S3 bucket

Another CLI command I ran was aws s3 ls s3://dray-bucket which returned 2025-08-09 04:17:33 155578 wallapp.jpg 2025-08-09 04:17:33 103333 wallapp2.jpeg

# Uploading objects to S3

To upload a new file to my bucket, I first ran the command sudo touch /tmp/test.txt This command creates an empty file

The second command I ran was aws s3 cp /tmp/test.txt s3://dray-bucket This command will copy the empty file to the bucket.

The third command I ran was aws s3 ls s3://dray-bucket which validated that its been copied successfully.

# The place to learn & showcase your skills

Check out nextwork.org for more projects