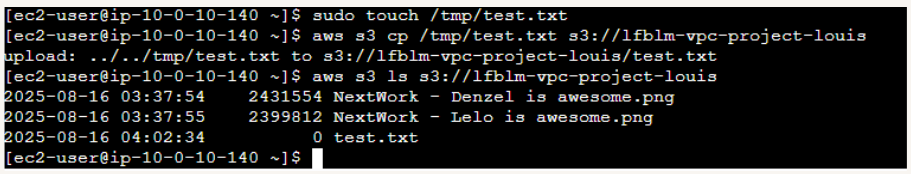
nextwork.org

Access S3 from a VPC

Louis Moyo



L
Louis Moyo
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private virtual network in AWS where you can launch resources like EC2 securely. It's useful because it gives control over IP ranges, subnets, and traffic flow.

How I used Amazon VPC in this project

I used Amazon VPC to create a new VPC with a public subnet and then launched an EC2 instance inside it, giving me a secure environment to connect and interact with AWS services.

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

One thing I didn't expect in this project was how simple it was to connect an EC2 instance to S3 using the AWS CLI after configuring access keys.

This project took me...

This project took me about 45 minutes to complete, including setting up the VPC, launching the EC2 instance, and connecting it to the S3 bucket.

In the first part of my project...

Step 1 - Architecture set up

I'm creating a VPC with a subnet, route table, security group, and NACL, then launching an EC2 instance in that subnet and attaching the SG. This gives me a controlled sandbox for secure access to S3."

Step 2 - Connect to my EC2 instance

I will be connecting directly to my EC2 instance in the VPC using EC2 Instance Connect. This will give me terminal access so I can run commands and interact with AWS services from inside my instance.

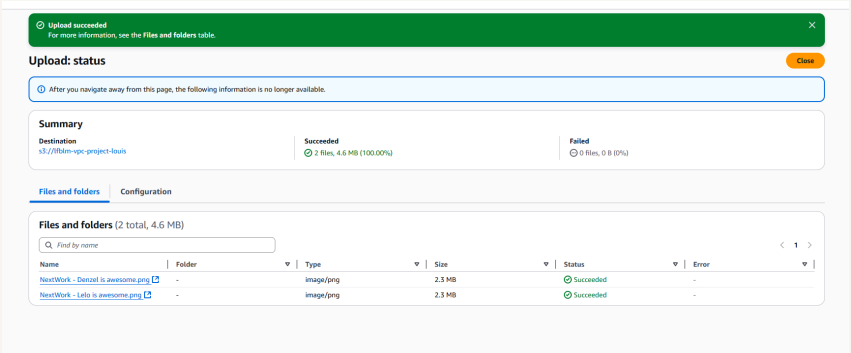
Step 3 - Set up access keys

I created access keys to give my EC2 instance credentials for connecting to my AWS environment. This lets the instance authenticate and securely access AWS services using the CLI.

Architecture set up

I started my project by launching a VPC, a public subnet, and an EC2 instance. I enabled a public IP and created a security group for SSH.

I also set up an S3 bucket and uploaded 2 files into it so I can later access and manage them from my EC2 instance using the AWS CLI.



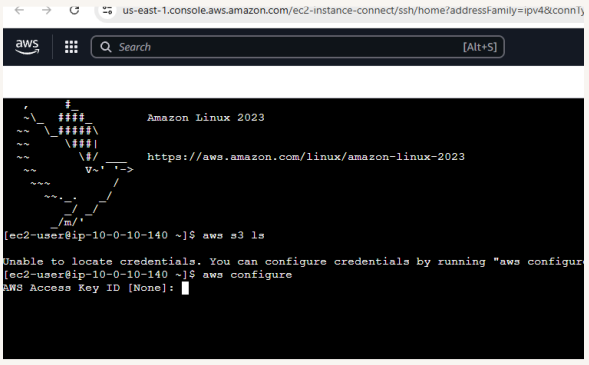
Louis Moyo
NextWork Student

Running CLI commands

AWS CLI is a command line tool that lets me manage AWS services using commands instead of the console.

The first command I ran was aws s3 ls. This command is used to list all the S3 buckets in my account and confirm that my EC2 instance can access AWS services through the CLI.

The second command I ran was aws configure. This command is used to set up my AWS CLI by providing the access key, secret key, region, and output format for authentication and configuration.



Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured the AWS CLI using the aws configure command, which set my access keys, region, and output format.

Access keys are a pair of credentials (Access Key ID and Secret Access Key) used to authenticate programmatic access to AWS services through the CLI or SDKs.

Secret access keys are like the password to the access key which is like a username. They must be kept safe because they allow programmatic access to AWS services through the CLI or SDKs.

Best practice

Although I'm using access keys in this project, a best practice alternative is to use IAM roles with temporary credentials, which are more secure and automatically managed by AWS.

In the second part of my project...

Step 4 - Set up an S3 bucket

I will be creating an S3 bucket and uploaded 2 files into it. This bucket will be used to practice accessing objects from my EC2 instance using the AWS CLI and to confirm my credentials are working.

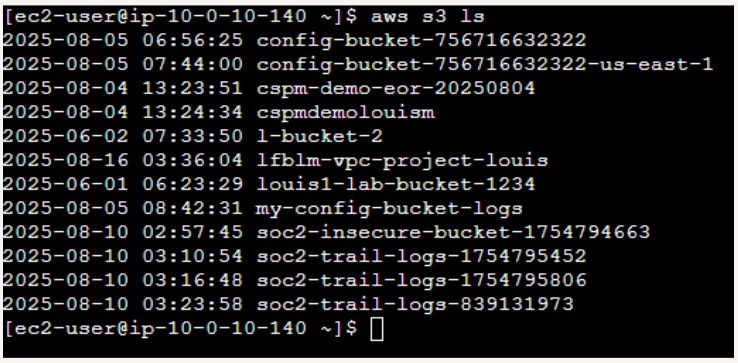
Step 5 - Connecting to my S3 bucket

I also set up an S3 bucket and uploaded 2 files into it so I can later access and manage them from my EC2 instance using the AWS CLI.

Connecting to my S3 bucket

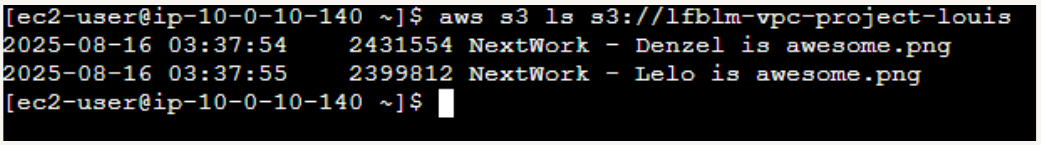
The first command I ran was aws s3 ls. This command is used to list all the S3 buckets in my account and confirm that my EC2 instance can access AWS services through the CLI.

When I ran the command aws s3 ls again, the terminal responded with a list of my S3 buckets. This indicated that my EC2 instance was correctly configured and able to access my AWS environment.



Connecting to my S3 bucket

Another CLI command I ran was aws s3 ls s3://lfblm-vpc-project-louis, which returned the list of objects stored in my S3 bucket along with their file sizes and timestamps

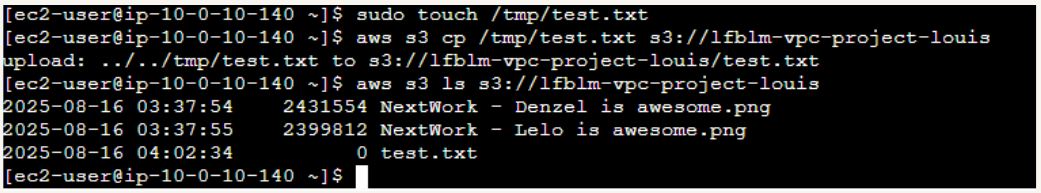


Uploading objects to S3

To upload a new file to my bucket, I first ran the command aws s3 cp filename.png s3://lfblm-vpc-project-louis/. This command creates a copy of my local file in the S3 bucket.

The second command I ran was aws s3 ls s3://lfblm-vpc-project-louis. This command will list all objects currently stored inside my S3 bucket.

The third command I ran was aws s3 ls s3://lfblm-vpc-project-louis again, which validated that my newly uploaded file appeared in the bucket alongside the existing objects.



The place to learn & showcase your skills

Check out nextwork.org for more projects