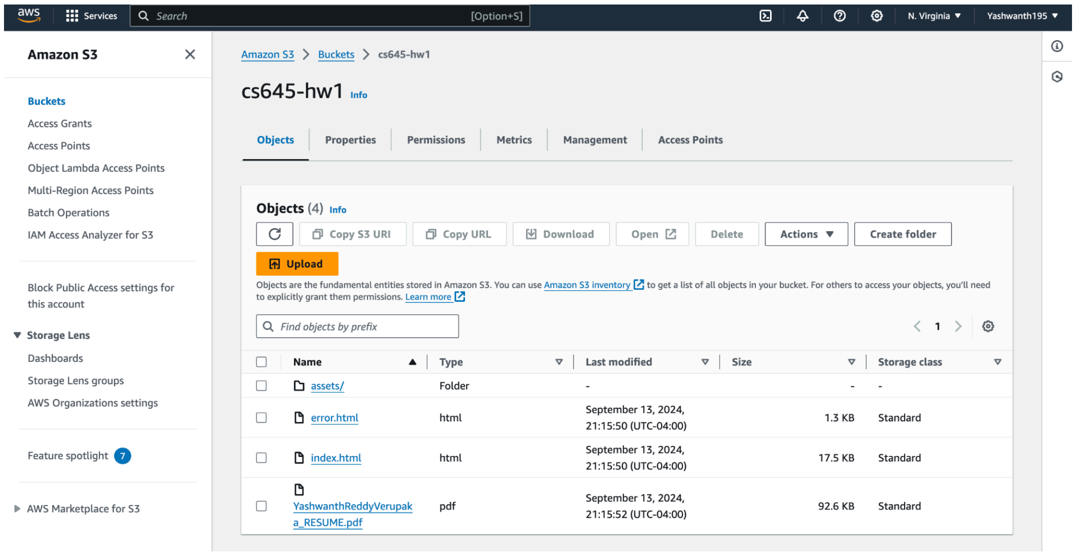
SWE645 ASSIGNMENT-1

Yashwanth Reddy Verupaka
G01455748

Steps involved for PART 1 - S3 Deployment:

- Create a bucket in S3 and add all the folders and files needed to the S3 bucket. A Pop up appears if everything uploads successfully.



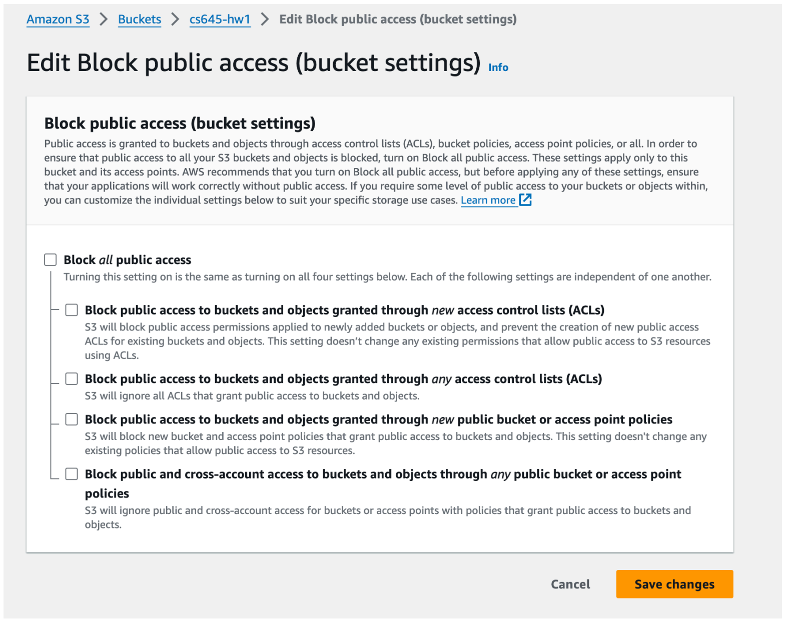
cs645-hw1 Info

Objects (4) Info

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

Name	Type	Last modified	Size	Storage class
assets/	Folder	-	-	-
error.html	html	September 13, 2024, 21:15:50 (UTC-04:00)	1.3 KB	Standard
index.html	html	September 13, 2024, 21:15:50 (UTC-04:00)	17.5 KB	Standard
YashwanthReddyVerupaka_RESUME.pdf	pdf	September 13, 2024, 21:15:52 (UTC-04:00)	92.6 KB	Standard

- Next allow public access to our files so that they can be accessed. Go to permissions menu of your bucket and disable "Block all public access"


Amazon S3 > Buckets > cs645-hw1 > Edit Block public access (bucket settings)
Cancel
Save changes

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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.

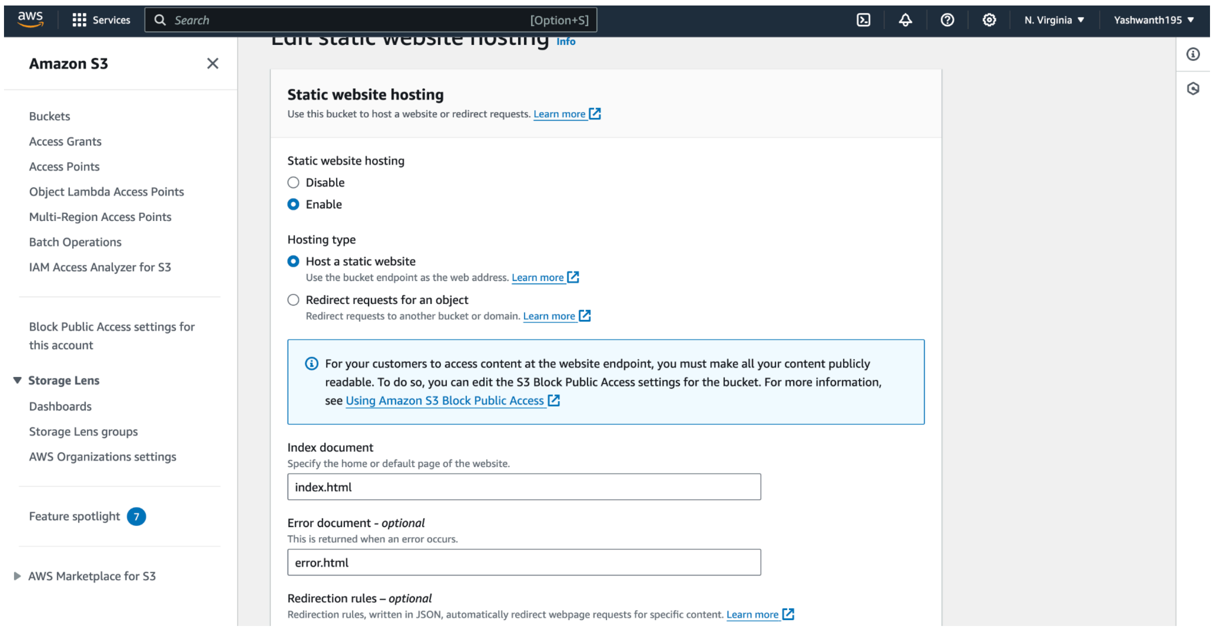
☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

- To publicly access your bucket add bucket policy to your bucket. Go to the permissions tab of your bucket edit under bucket policy
- Enter the bucket policy provided on the AWS site in the editor:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
    "Sid": "PublicReadGetObject",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::Bucket-name/*"
    }
    ]}
```

Replace “bucket name” with your own bucket name.

- Enable Static Web Hosting by enabling it in the properties tab. Also add the index and error html pages path in the block provided.



Static website hosting
Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Disable [✓ Enable]

Hosting type
[✓ Host a static website]
Use the bucket endpoint as the web address. Learn more
Redirect requests for an object
Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

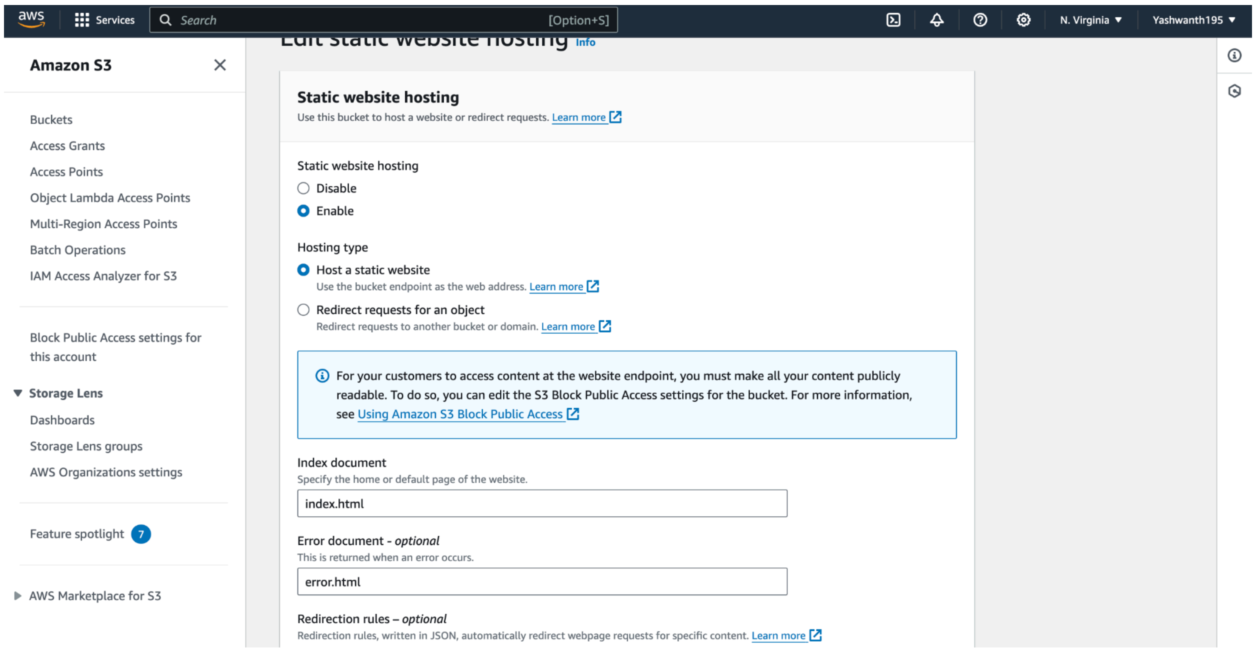
Index document
Specify the home or default page of the website.
index.html

Error document - *optional*
This is returned when an error occurs.
error.html

Redirection rules – *optional*
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more

- This generates a link that can be used to access the website.

Link to S3 deployment:- http://cs645-hw1.s3-website-us-east-1.amazonaws.com



Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Disable [✓ Enable]

Hosting type
[✓ Host a static website]
Use the bucket endpoint as the web address. Learn more
Redirect requests for an object
Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

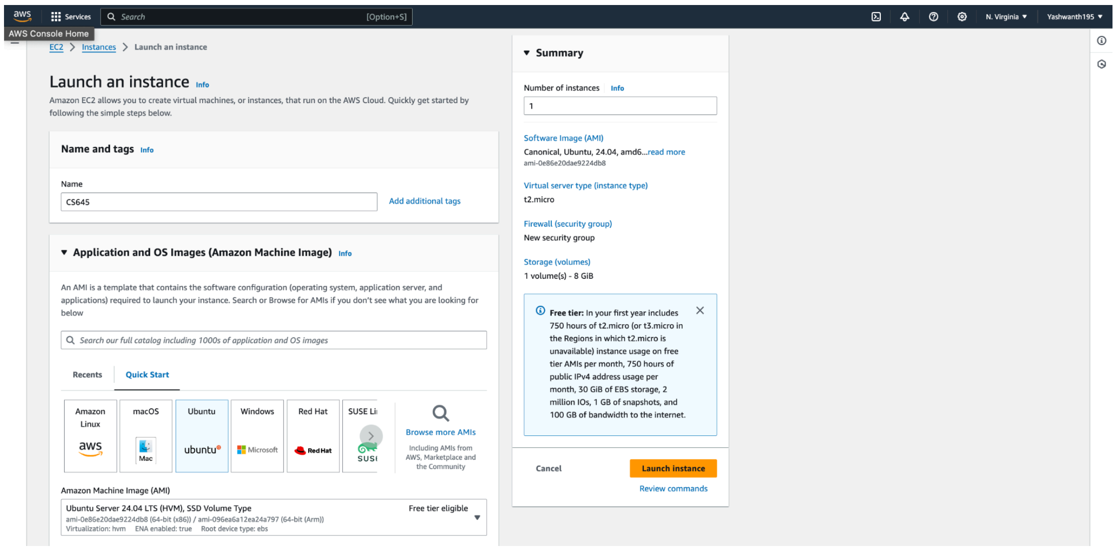
Index document
Specify the home or default page of the website.
index.html

Error document - *optional*
This is returned when an error occurs.
error.html

Redirection rules – *optional*
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more

Steps involved for PART 2 - EC2 Deployment:

- Create an EC2 instance on your AWS account. Select the AMI you want, I have chosen Ubuntu and set the instance type to t2.micro and give a desired name.



Launch an instance

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

Name: CS645

Application and OS Images (Amazon Machine Image)

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

Amazon Machine Image (AMI)
Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-0e86e20dae9224db8 (64-bit (x86)) / ami-096ea6a12ea24a797 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Summary

Number of instances: 1

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-0e86e20dae9224db8

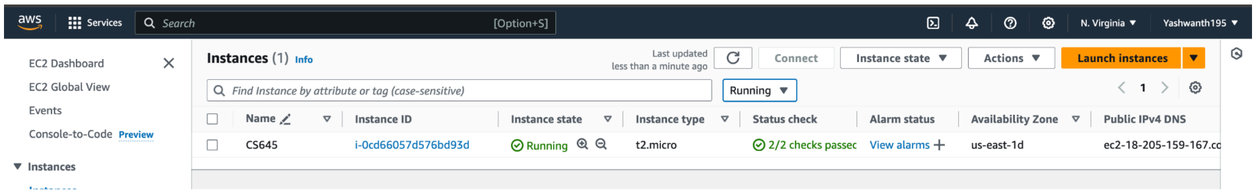
Virtual server type (instance type)
t2.micro

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.

- Create a key pair that can be used to access your instance.
- Also create a security group which allows us to set rules that control the traffic for your instance. Make sure to allow inbound traffic from Port 80(HTTP) and Port 22(SSH) to ensure that requests are served.



Instances (1) Info

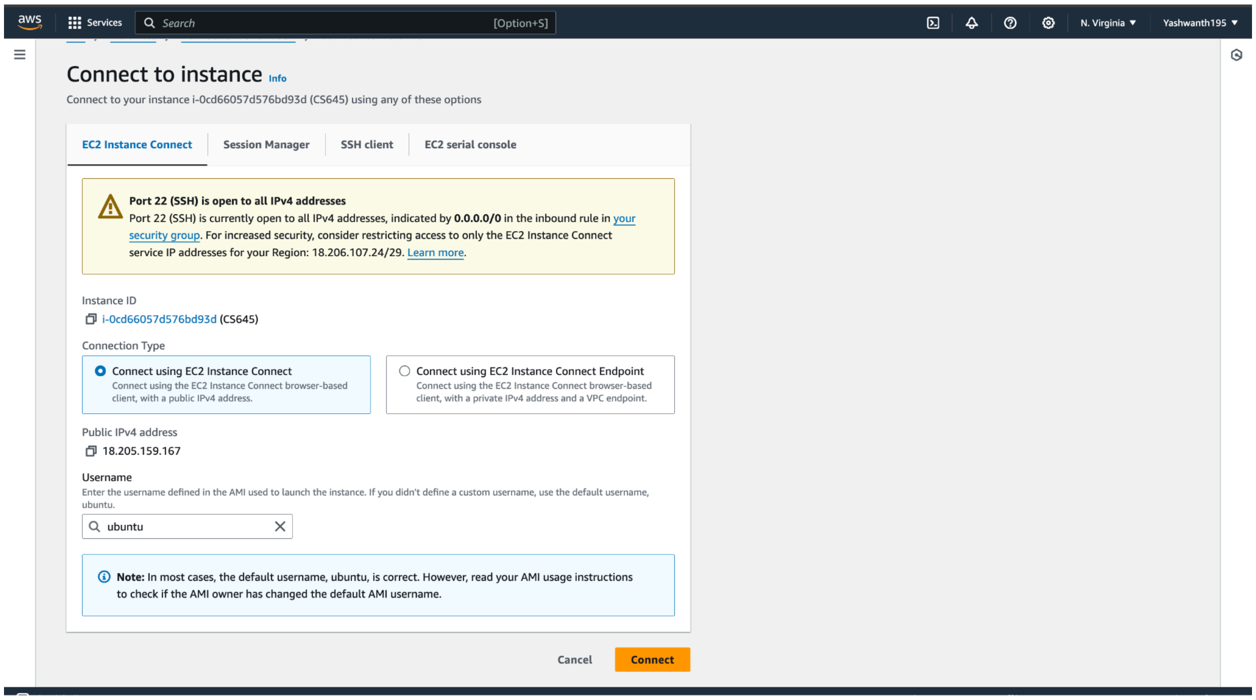
Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

Running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
CS645	i-0cd66057d576bd93d	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1d	ec2-18-205-159-167.cc

- Connect to this instance, by clicking on the "Connect" button at the bottom. You can set the username of the AMI or leave it as default which is ubuntu.



Connect to instance Info

Connect to your instance i-0cd66057d576bd93d (CS645) using any of these options

Port 22 (SSH) is open to all IPv4 addresses
Port 22 (SSH) is currently open to all IPv4 addresses, indicated by **0.0.0.0/0** in the inbound rule in your security group. For increased security, consider restricting access to only the EC2 Instance Connect service IP addresses for your Region: 18.206.107.24/29. Learn more.

Instance ID
i-0cd66057d576bd93d (CS645)

Connection Type
- [✓ Connect using EC2 Instance Connect] Connect using the EC2 Instance Connect browser-based client, with a public IPv4 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
18.205.159.167

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

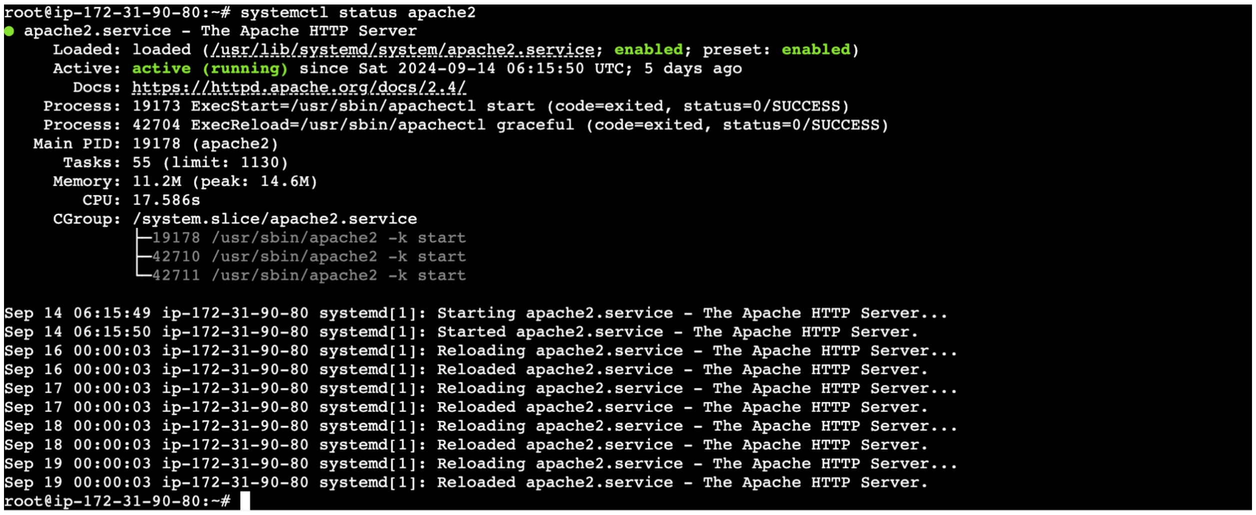
Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

- Once connected to the instance switch to root user by using the command.

Sudo su -

- Install the apache server and check if the server is installed.
  - **Command to install:** *sudo apt install apache2*
  - **Command to check:** *sudo ufw app list*
- Now, this server will have to disable its firewall.
  - **Command to diable firewall:** *sudo ufw allow 'Apache'*

- Check if the apache server is running by using the command.
    - **Command to check status:** *sudo systemctl status apache2*



```
root@ip-172-31-90-80:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-09-14 06:15:50 UTC; 5 days ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 19173 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Process: 42704 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
   Main PID: 19178 (apache2)
      Tasks: 55 (limit: 1130)
     Memory: 11.2M (peak: 14.6M)
        CPU: 17.586s
     CGroup: /system.slice/apache2.service
             ├─19178 /usr/sbin/apache2 -k start
             ├─42710 /usr/sbin/apache2 -k start
             └─42711 /usr/sbin/apache2 -k start

Sep 14 06:15:49 ip-172-31-90-80 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Sep 14 06:15:50 ip-172-31-90-80 systemd[1]: Started apache2.service - The Apache HTTP Server.
Sep 16 00:00:03 ip-172-31-90-80 systemd[1]: Reloading apache2.service - The Apache HTTP Server...
Sep 16 00:00:03 ip-172-31-90-80 systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
Sep 17 00:00:03 ip-172-31-90-80 systemd[1]: Reloading apache2.service - The Apache HTTP Server...
Sep 17 00:00:03 ip-172-31-90-80 systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
Sep 18 00:00:03 ip-172-31-90-80 systemd[1]: Reloading apache2.service - The Apache HTTP Server...
Sep 18 00:00:03 ip-172-31-90-80 systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
Sep 19 00:00:03 ip-172-31-90-80 systemd[1]: Reloading apache2.service - The Apache HTTP Server...
Sep 19 00:00:03 ip-172-31-90-80 systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
root@ip-172-31-90-80:~# 
```

- Now upload all the files needed for deployment from your local machine to your EC2 instance. Instead of sending each file I have zipped the entire folder and sent it as a file.Use the following command in your local machine to server copy the files.
    - *scp -i CS645-key.pem /Users/yashwanthverupaka/Desktop/Working-645.zip ubuntu@ec2-18-205-159-167.compute-1.amazonaws.com:*

      ec2-18-205-159-167.compute-1.amazonaws.com*: is my* **Public IPv4 DNS**

- Once files are copied to the server unzip the folder.
- Once unzipped cd into the folder and move all the files into '/var/www/html/' folder
    - **Command to move files:** mv * /var/www/html/
- Once all files are present and the server is active, you must be able to access your page using the public IPv4 DNS link.

  Link to EC2 deployment:- ec2-18-205-159-167.compute-1.amazonaws.com

LINKS to DEPLOYMENTS:

➔ **S3 Deployment:** http://cs645-hw1.s3-website-us-east-1.amazonaws.com
➔ **EC2 deployment:** ec2-18-205-159-167.compute-1.amazonaws.com