

AMITY SCHOOL OF ENGINEERING & TECHNOLOGY



(Academic Year 2022-23)

LAB- 5

EC2 Instances

Student Name: Vikas Rajbhar

Class: B. Tech CSE Semester: 7

Enrolment Number: A70405219037

Faculty In-charge

{Department of CSE}

ASET, AUM

AIM OF THE EXPERIMENT:

Perform the following tasks:

1. Create an EC2 Instance
2. Demonstrate the working of static and dynamic website through EC2
3. Shift files from S3 to EC2
4. Shift files from EC2 to S3

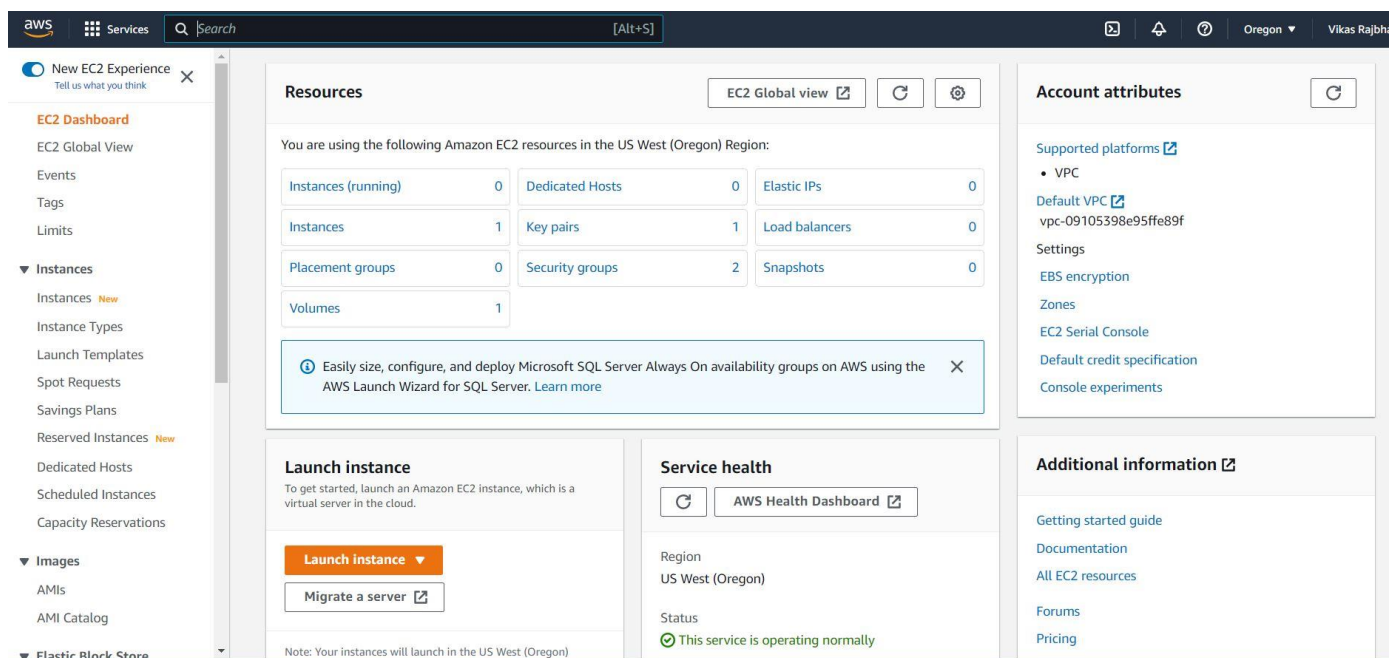
THEORY:

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

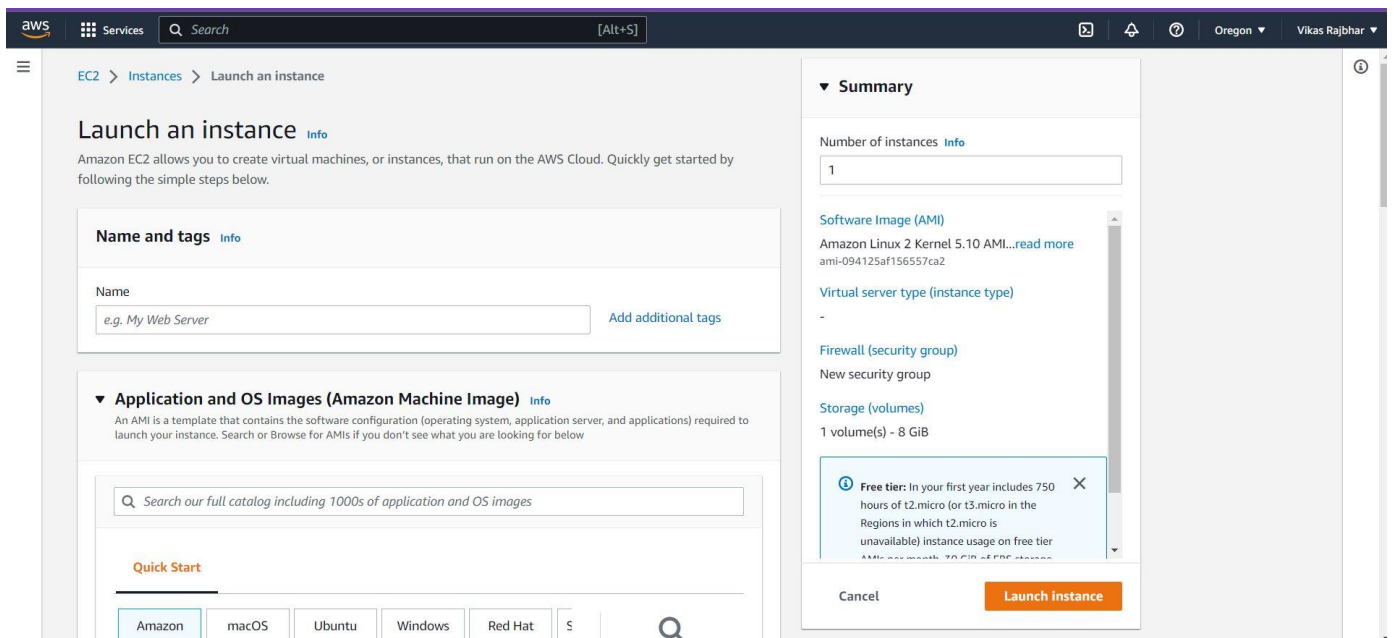
Creating an EC2 Instance

Launching Amazon EC2 Linux Instances:

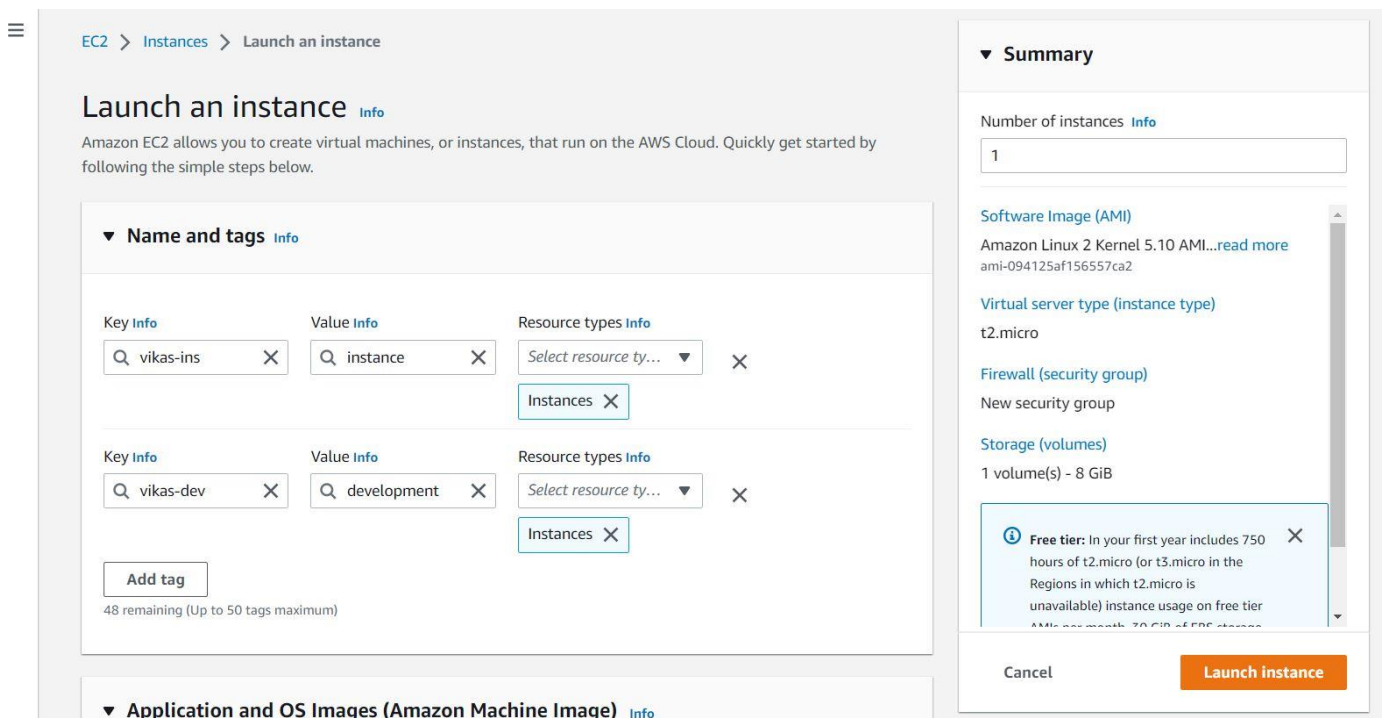
1. Open the Amazon EC2 console.



2. From the EC2 console dashboard, in the **Launch instance** box, choose **Launch instance**, and then choose **Launch instance** from the options that appear.



3. Under **Name and tags**, for **Name**, enter a descriptive name for your instance.



4. Under **Application and OS Images (Amazon Machine Image)**, do the following:
 - a. Choose **Quick Start**, and then choose Amazon Linux. This is the operating system (OS) for your instance.
 - b. From **Amazon Machine Image (AMI)**, select an HVM version of Amazon Linux 2. Notice that these AMIs are marked **Free tier eligible**. An *Amazon Machine Image (AMI)* is a basic configuration that serves as a template for your instance.

aws Services Search [Alt+S] Oregon Vikas Rajbhar

EC2 > Instances > Launch an instance > AMIs

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Quickstart AMIs (47) Commonly used AMIs

My AMIs (0) Created by me

AWS Marketplace AMIs (6576) AWS & trusted third-party AMIs

Community AMIs (500) Published by anyone

Refine results

Clear all filters

☐ Free tier only info

OS category

☐ All Linux / Unix

All products (47 filtered, 47 unfiltered)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-094125af156557ca2 (64-bit (x86)) / ami-0f96a89e4a6cf08cc (64-bit (Arm))

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Platform: amazon Root device type: ebs Virtualization: hvm ENA enabled: Yes

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

aws Services Search [Alt+S] Oregon Vikas Rajbhar

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

AMI from catalog Quick Start

Amazon Machine Image (AMI)

amzn2-ami-kernel-5.10-hvm-2.0.20221103.3-x86_64-gp2
ami-094125af156557ca2

Free tier eligible
Verified provider

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

Catalog	Published	Architecture	Virtualization	Root device type	ENA Enabled
Quickstart AMIs	2022-11-14T23:11:48.000Z	x86_64	hvm	ebs	Yes

Summary

Number of instances **Info**
1

Software Image (AMI)
Amazon Linux 2 AMI (HVM) - Ker...read more
ami-094125af156557ca2

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

Cancel **Launch instance**

Instance type Info

- Under **Instance type**, from the **Instance type** list, you can select the hardware configuration for your instance. Choose the t2.micro instance type, which is selected by default.

Instance type Info

Instance type

t2.micro **Free tier eligible**

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

Compare instance types

- Under **Key pair (login)**, for **Key pair name**, choose the key pair that you created when getting set up.


▼ **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*

vikasrajbhar

▼

 [Create new key pair](#)

- Next to **Network settings**, choose **Edit**. For **Security group name**, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up using the following steps:
 - Choose **Select existing security group**.
 - From **Common security groups**, choose your security group from the list of existing security groups.

▼ **Network settings** [Info](#) Edit

Network [Info](#)

vpc-09105398e95ffe89f

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

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

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

 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.

×

▼ **Summary**

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...[read more](#)

ami-094125af156557ca2

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 are subject to 750 CPU hours of free usage.

×

Cancel

Launch instance

- Keep the default selections for the other configuration settings for your instance.
- Review a summary of your instance configuration in the **Summary** panel, and when you're ready, choose **Launch instance**.

▼ Configure storage Info

Advanced

1x 8 GiB gp2 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

0 x File systems Edit

► Advanced details Info

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

Cancel Launch instance

10. A confirmation page lets you know that your instance is launching. Choose **View all instances** to close the confirmation page and return to the console.

EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-0d36fb55217e4d7a4)

Launch log

Next Steps

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Create billing alerts

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect to instance

Learn more

Connect an RDS database

New

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Connect an RDS database

Create a new RDS database

Learn more

11. On the **Instances** screen, you can view the status of the launch. After the instance starts, its state changes to running and it receives a public DNS name.

12. It can take a few minutes for the instance to be ready for you to connect to it.

aws Services Search [Alt+S]

New EC2 Experience Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances (1) Info

Find instance by attribute or tag (case-sensitive)

Connect

Instance state

Actions

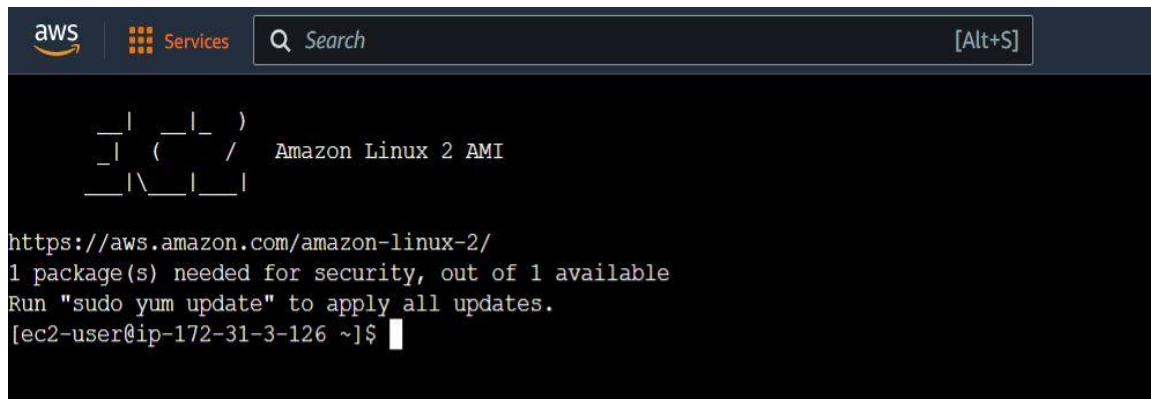
Launch instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
	-	i-0d36fb55217e4d7a4	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	ec2-54-200-44-112

Deploying Websites through EC2

Static

1. SSH into EC2 Instance

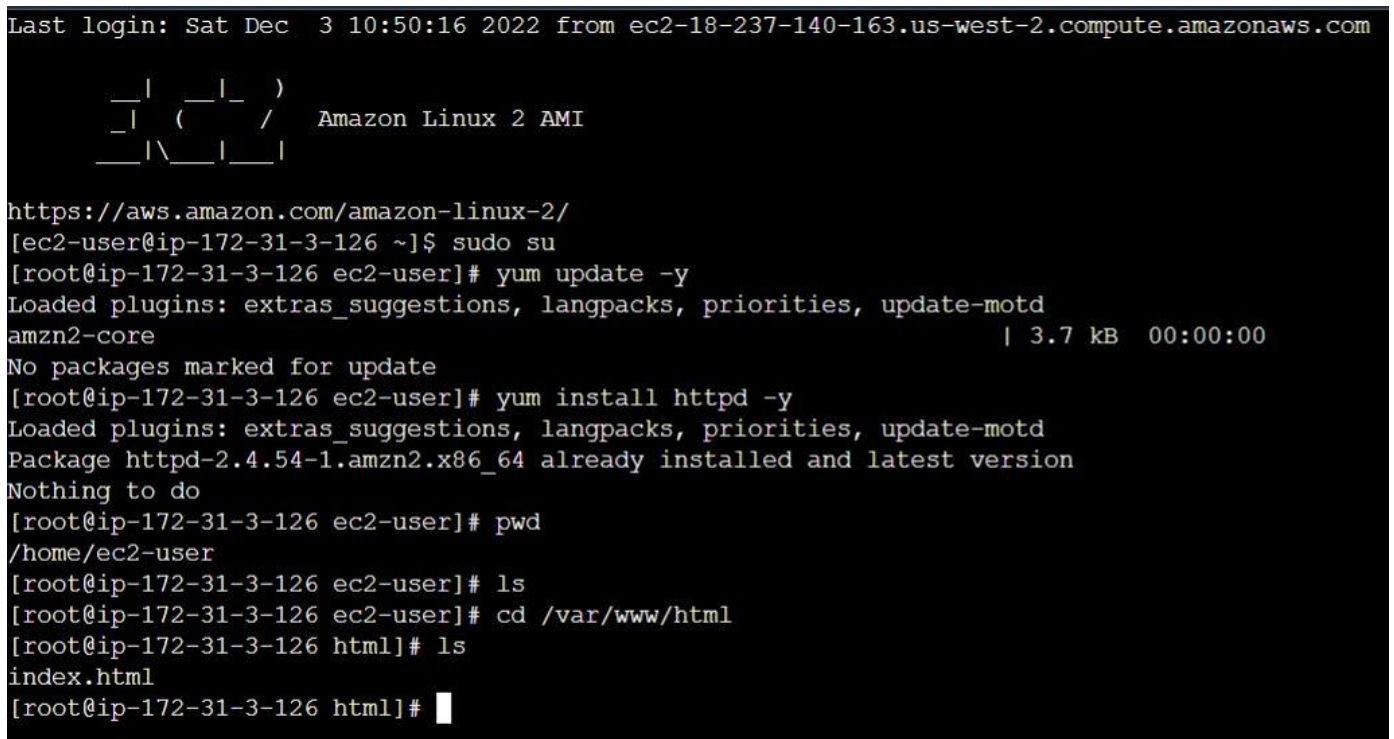


```
aws Services Search [Alt+S]

__|  __|_ )
_| (  _/   Amazon Linux 2 AMI
__|\__|__|

https://aws.amazon.com/amazon-linux-2/
1 package(s) needed for security, out of 1 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-3-126 ~]$
```

2. Elevate your privileges: **sudo su**
3. Update all the packages on the instance: **yum update -y**
4. Install an Apache webserver: **yum install httpd -y**
5. Navigate to **/var/www/html**

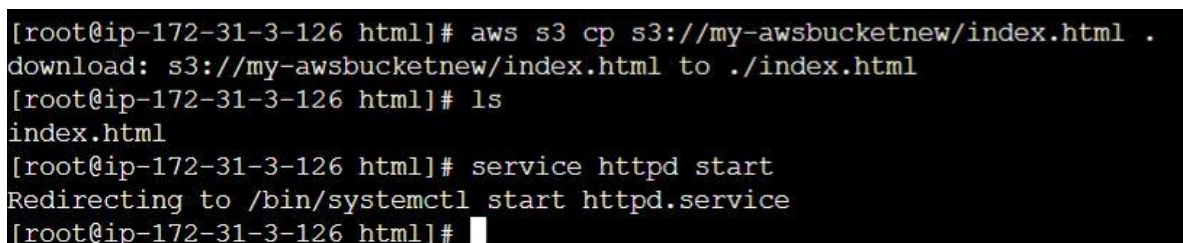


```
Last login: Sat Dec 3 10:50:16 2022 from ec2-18-237-140-163.us-west-2.compute.amazonaws.com

__|  __|_ )
_| (  _/   Amazon Linux 2 AMI
__|\__|__|

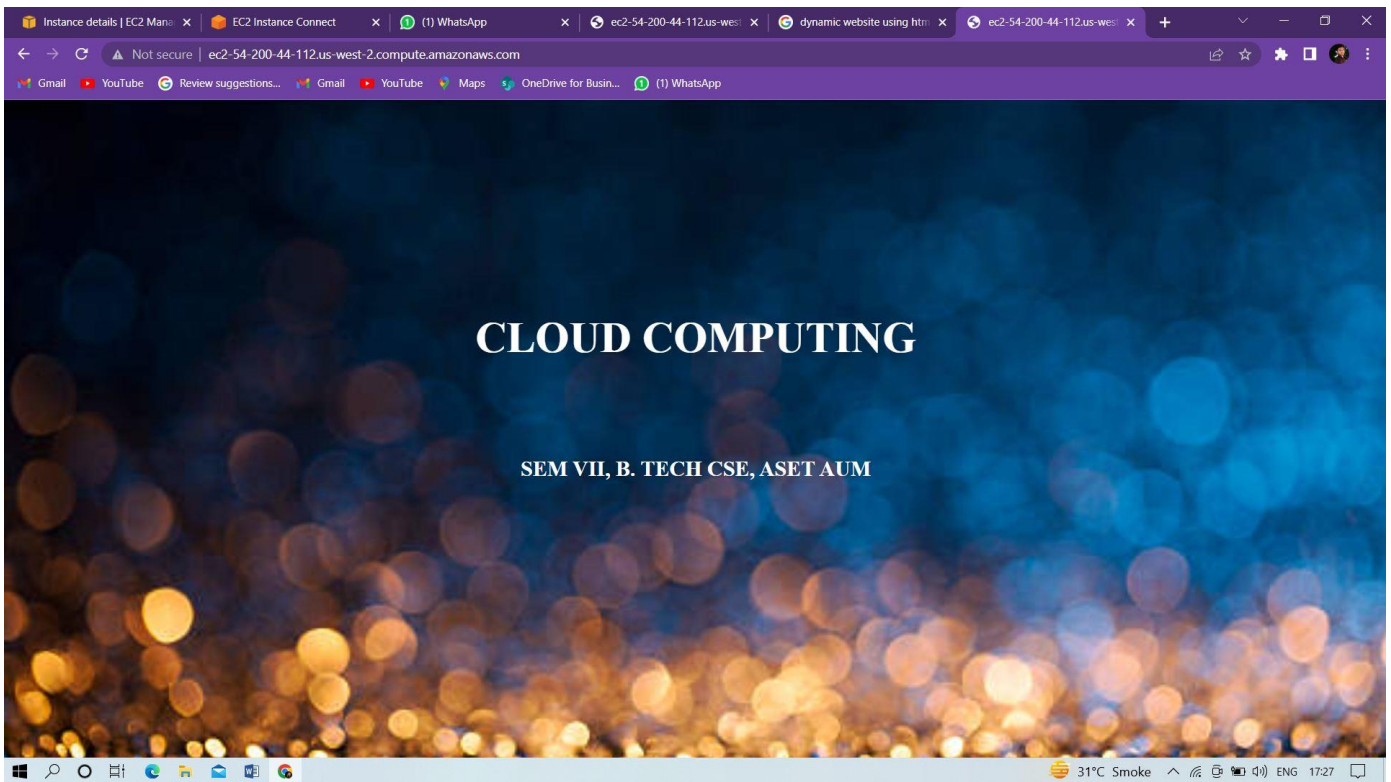
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-3-126 ~]$ sudo su
[root@ip-172-31-3-126 ec2-user]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core | 3.7 kB 00:00:00
No packages marked for update
[root@ip-172-31-3-126 ec2-user]# yum install httpd -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Package httpd-2.4.54-1.amzn2.x86_64 already installed and latest version
Nothing to do
[root@ip-172-31-3-126 ec2-user]# pwd
/home/ec2-user
[root@ip-172-31-3-126 ec2-user]# ls
[root@ip-172-31-3-126 ec2-user]# cd /var/www/html
[root@ip-172-31-3-126 html]# ls
index.html
[root@ip-172-31-3-126 html]#
```

6. Copy the index.html file from S3 bucket to EC2 instance:
s3://my-awsbucketnew/index.html .
7. Start the webserver: **service httpd start**



```
[root@ip-172-31-3-126 html]# aws s3 cp s3://my-awsbucketnew/index.html .
download: s3://my-awsbucketnew/index.html to ./index.html
[root@ip-172-31-3-126 html]# ls
index.html
[root@ip-172-31-3-126 html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-3-126 html]#
```

8. Navigate back to the EC2 dashboard in the AWS console and copy the public DNS (IPv4) of the instance. Paste the address with `http://` at the start.



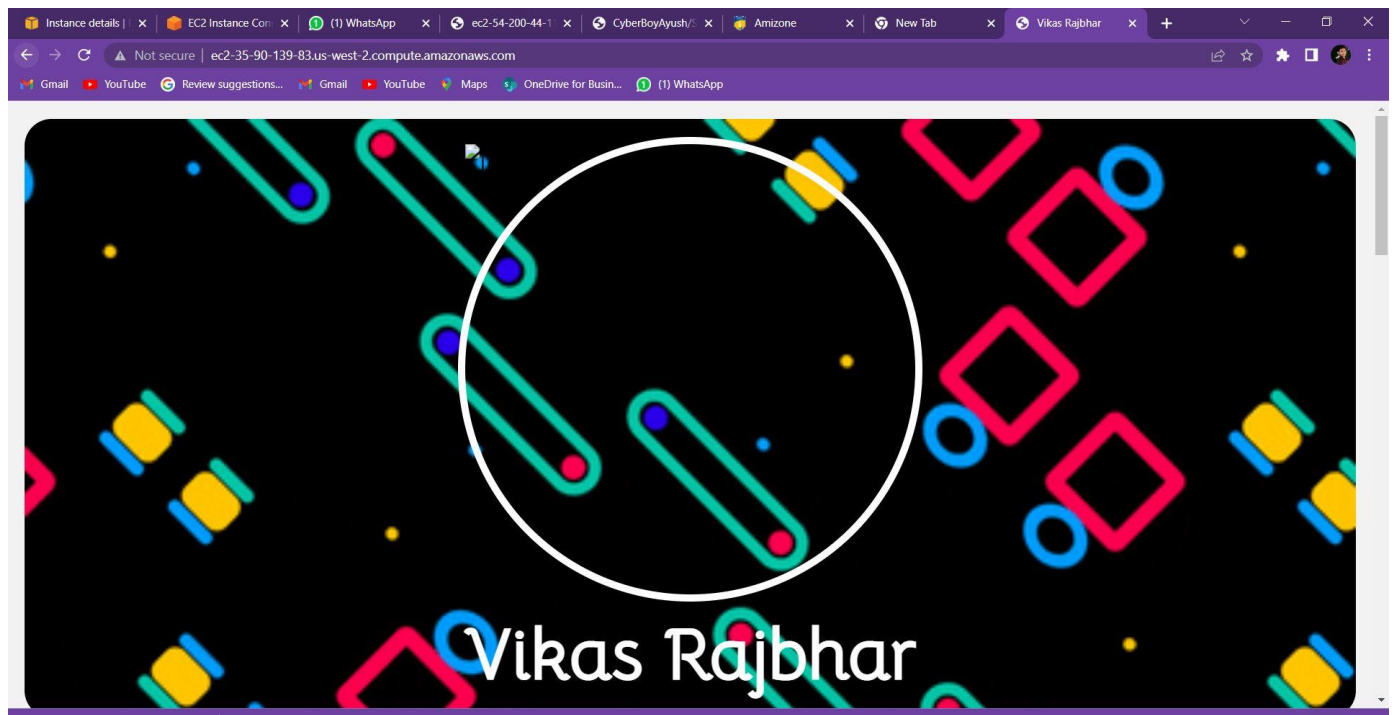
Dynamic

The steps to deploy a dynamic website are like the steps mentioned previously, except for copying the files and folders.

The `--recursive` flag is used in the copying command to recursively copy the files from directories, thus, copying whole directories. Copy all the files and folders into `/var/www/html`

```
1. aws s3 cp s3://vikas-website/ . --recursive
```

```
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-12-139 ~]$ sudo su
[root@ip-172-31-12-139 ec2-user]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
No packages marked for update
[root@ip-172-31-12-139 ec2-user]# yum install httpd -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Package httpd-2.4.54-1.amzn2.x86_64 already installed and latest version
Nothing to do
[root@ip-172-31-12-139 ec2-user]# ls
[root@ip-172-31-12-139 ec2-user]# cd /var/www/html
[root@ip-172-31-12-139 html]# ls
[root@ip-172-31-12-139 html]# aws s3 cp s3://vikasbucket1278/vikas-website/ . --recursive
download: s3://vikasbucket1278/vikas-website/index.html to ./index.html
download: s3://vikasbucket1278/vikas-website/style.css to ./style.css
[root@ip-172-31-12-139 html]# systemctl start httpd
bash: systemctl: command not found
[root@ip-172-31-12-139 html]# ls
index.html  style.css
[root@ip-172-31-12-139 html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-12-139 html]#
```

Shifting Files

In AWS technical terms.

Copying files from **EC2 to S3** is called **Uploading** the file

Copying files from **S3 to EC2** is called **Downloading** the files

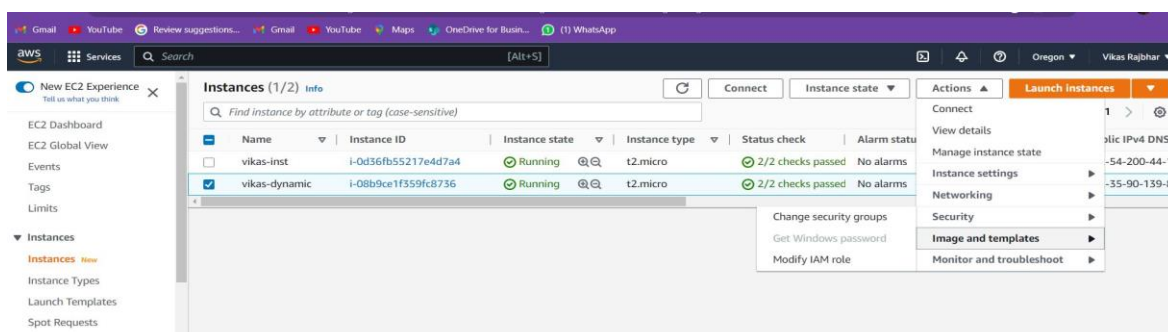
- **S3 to EC2**

Prerequisites

1. An EC2 instance should exist where we would be performing actions on the S3 bucket
2. Ensure that AWS CLI is installed on the EC2 instance
3. An S3 bucket with some files to use for the transfer

Perform the following steps to add an instance profile to the EC2 instance to grant required permissions to the instance:

1. Log in to the AWS console
2. Navigate to the EC2 details page
3. Select the instance we want to add the instance profile (IAM role) to, click on the Actions drop-down menu, and click on the "Modify IAM role" option



4. Select an existing IAM role from the drop-down menu (or create a new one if needed) and click on the "Save" button.

EC2 > Instances > i-08b9ce1f359fc8736 > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID
 i-08b9ce1f359fc8736 (vikas-dynamic)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

VikasNewRole

[Create new IAM role](#)

Cancel [Update IAM role](#)

Adding required S3 permissions to the IAM Instance Profile role

Perform the following steps to add required permission to the IAM instance profile role to allow the instance to perform actions on the S3 bucket

1. Navigate to the IAM details page and click on the roles menu and select the role that was attached to the EC2 instance

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report

Roles (12) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

<input type="checkbox"/>	Role name	Trusted entities	Last act...
<input type="checkbox"/>	AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application-autoscaling (Service-Linked Role)	19 minutes ago
<input type="checkbox"/>	AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	1 hour ago
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
<input type="checkbox"/>	IAMReadOnly	AWS Service: ec2	-
<input type="checkbox"/>	rds-monitoring-role	AWS Service: monitoring.rds	5 days ago
<input type="checkbox"/>	s3curr_role_for_my-awsbucketnew	AWS Service: s3	45 days ago

[Delete](#) [Create role](#)

2. Click on the "Add permissions" button and select the "Attach policies" option
3. Filter and attach the AmazonS3FullAccess policy from the list and click on the Attach policies button

Allows EC2 instances to call AWS services on your behalf.

Summary [Edit](#)

Creation date December 03, 2022, 16:03 (UTC+05:30)	ARN arn:aws:iam::981873548788:role/vikas-iam	Instance profile ARN arn:aws:iam::981873548788:instance-profile/vikas-iam
Last activity 26 minutes ago	Maximum session duration 1 hour	

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

[Filter policies by property or policy name and press enter.](#)

<input type="checkbox"/>	Policy name ↗	Type	Description
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t

Copying files from the S3 bucket to the EC2 instance

Perform the following steps to copy a file from an S3 bucket to the EC2 instance:

1. SSH into the EC2 instance (using PuTTY)
2. Run `aws s3 cp <S3_Object_URI> <Local_File_Path>` to copy files from S3 bucket to the EC2 instance

```
[root@ip-172-31-12-139 html]# aws s3 cp s3://vikasbucket1278/vikas-website/index.html .
download: s3://vikasbucket1278/vikas-website/index.html to ./index.html
[root@ip-172-31-12-139 html]# ls
index.html  style.css
[root@ip-172-31-12-139 html]#
```

- **EC2 to S3**

To move files from EC2 to S3, we simply execute the following command with the previously mentioned IAM roles still being placed under the instances.

1. To list the files, present in the bucket: `aws s3 ls s3://vikasbucket1278`
2. To move a file from EC2 to S3:

```
[root@ip-172-31-12-139 html]# aws s3 ls s3://vikasbucket1278
PRE vikas-website/
[root@ip-172-31-12-139 html]# ls
index.html  style.css
[root@ip-172-31-12-139 html]#
```