



**BHARATI VIDYAPEETH'S
INSTITUTE OF COMPUTER APPLICATIONS &
MANAGEMENT**

(Affiliated to Guru Gobind Singh
Indraprastha University, Approved by
AICTE, New Delhi)

**Cloud Computing Lab
(MCA-265)**

Practical File

Submitted To:

Dr. Arpita Nagpal
(Assistant Professor)

Submitted By:

Sandeep Wadhawan (01411604422)
MCA 3rd Sem, Sec - 1

INDEX

<u>S.No.</u>	<u>Description</u>	<u>BTL</u>	<u>CO</u>	<u>Date</u>	<u>Sign. Of teacher</u>
P1.0	Assume you have started your own entrepreneur and your work is increasing at a high speed, you employ more workers. Now you will take the help of cloud providers. Give the details of different providers.			04-08-2023	
P2.1	Install the VMWare ESXi 6.5 either in VMWare Workstation or Oracle Virtual Box.	2	Demonstrate the cloud platform on an appropriate tool.	02-09-2023	
P2.2	Install multiple guest OS like Ubuntu Server, CentOS, Fedora etc. and manage the guest OS.				
P3.1	Find a procedure to set up an account with AWS, services it offers. Support your procedure with screenshots.	3	Apply virtualization n in clouds	06-09-2023	
P3.2	Demonstrate the steps with screenshots to add a new instance and create a virtual machine in Amazon Web Service using EC2.				
P4.0	Suppose you are an AWS cloud consultant. Mr. Hemant came to you with following constraints: 1. He needs a remote desktop Login of the virtual machine you created using EC2 instance. 2. Need to create a webpage using Webserver IIS to demonstrate the importance of cloud.	4	Distinguish between at least two cloud-based platform	11-09-2023	

Cloud Computing

P5.0	Assume, you are technical advisor in your organization. The organization's vision is to provide use the cloud services in AWS. You are directed to give Roles, authentication and authorizations to employees using a particular service of cloud.	5	Choose and implement best security practices of cloud	19-09-2023	
P6.0	Demonstration Elastic Load balancing using ECS in AWS Tasks Step 1: Configure a target group Step 2: Register targets Step 3: Configure a load balancer and a listener Step 4: Test the load balancer	6	Create automation on load balancing in cloud.	11-10-2023	

P1.0:- Assume you have started your own entrepreneur and your work is increasing at a high speed, you employ more workers. Now you will take the help of cloud providers. Give the details of different providers.

Solution:-

Here are details of 10 different cloud service providers:

1. Amazon Web Services (AWS):

- AWS is a comprehensive and widely-used cloud platform offering a vast array of services, including computing, storage, databases, machine learning, analytics, and more. It is known for its scalability and reliability, making it popular among startups and enterprises alike.

2. Microsoft Azure:

- Azure is Microsoft's cloud computing platform that provides services for computing, analytics, networking, storage, and more. It integrates well with Microsoft products and services, making it a preferred choice for organizations in the Microsoft ecosystem.

3. Google Cloud Platform (GCP):

- GCP is Google's cloud offering that includes services for computing, data analytics, machine learning, storage, and networking. It's known for its powerful data processing capabilities and AI/ML services.

4. IBM Cloud:

- IBM Cloud offers a range of cloud services, including infrastructure, platform, and software services. It is particularly popular among enterprises that require advanced AI and data analytics capabilities.

5. Oracle Cloud:

- Oracle Cloud provides cloud infrastructure, platform, and application services tailored to enterprise needs. It specializes in database management and enterprise-grade applications.

6. Alibaba Cloud:

- Alibaba Cloud is the cloud computing arm of Alibaba Group, catering to businesses in China and globally. It offers a wide range of cloud services, including computing, storage, and big data processing.

7. DigitalOcean:

- DigitalOcean is a developer-friendly cloud provider known for its simplicity and ease of use. It focuses on providing scalable virtual servers (droplets) and other cloud services geared towards developers and small to medium-sized businesses.

8. Vultr:

- Vultr is another cloud provider popular among developers due to its straightforward pricing and high-performance virtual machines. It offers cloud computing instances in multiple locations worldwide.

9. Linode:

- Linode is a well-established cloud provider known for its reliable virtual servers and straightforward pricing. It caters to developers and businesses of various sizes.

10. Rackspace:

- Rackspace is a managed cloud provider that offers a range of cloud services, including public, private, and hybrid cloud solutions. They specialize in providing support and managed services to businesses looking to offload cloud infrastructure management.

Each of these cloud providers has its strengths and target markets, so it's essential to consider specific requirements and budget while choosing the right cloud provider for the business.

P2.1:- Install the VMWare ESXi 6.5 either in VMWare Workstation or Oracle Virtual Box.

Solution:-

Installing VMware ESXi 6.5 within a virtualization platform like VMware Workstation or Oracle VirtualBox can be helpful for testing and learning purposes, but it's important to note that ESXi itself is a hypervisor that is typically installed on physical hardware to create and manage virtual machines. Running ESXi inside another virtualization platform creates nested virtualization, which may have some limitations.

Here are the basic steps to install ESXi 6.5 within VMware Workstation or Oracle VirtualBox:

Prerequisites:

- You need a copy of the VMware ESXi 6.5 ISO image.
- Make sure your host machine has hardware virtualization support (VT-x/AMD-V) enabled in the BIOS/UEFI settings.
- Allocate sufficient resources (CPU cores, RAM, and storage) to the virtual machine running ESXi.

Instructions:

1. In VMware Workstation:

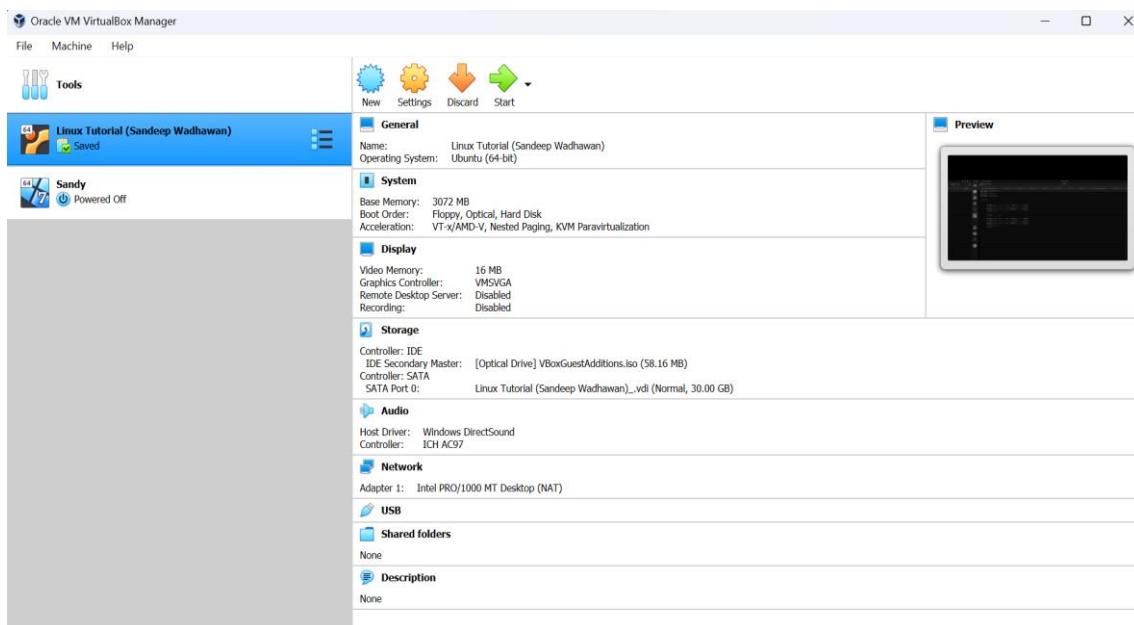
- a. Open VMware Workstation and click "File" > "New Virtual Machine."
- b. Choose "Custom (advanced)" and click "Next."
- c. Select "I will install the operating system later" and click "Next."
- d. Choose "Linux" and "Other Linux 2.6.x kernel 64-bit" as the guest operating system.
- e. Name the virtual machine and specify the location.
- f. Configure CPU, memory, and network settings as needed.
- g. In the "Select a Disk" window, choose "Use an existing virtual disk" and select the ESXi 6.5 ISO file.
- h. Finish the virtual machine creation wizard.
- i. Before powering on the virtual machine, go to "Edit virtual machine settings" and add a new hardware item: "New CD/DVD (SATA)." Choose "Use ISO image file" and select the ESXi 6.5 ISO.

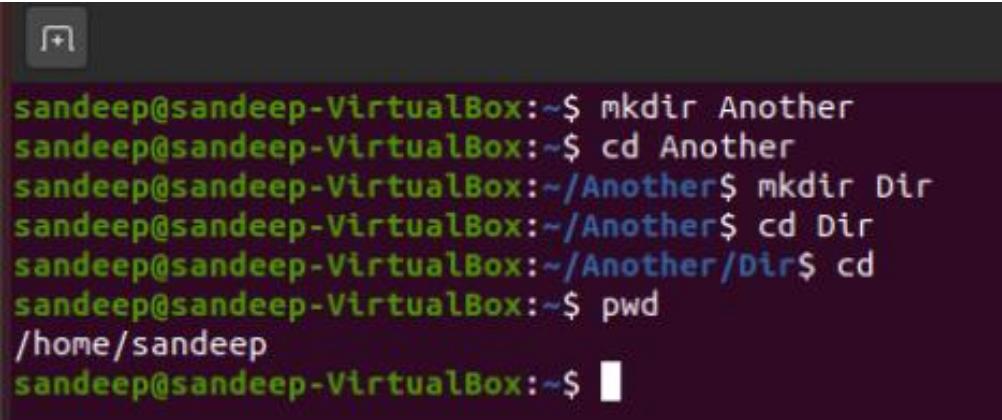
When you power on the virtual machine, it should boot from the ESXi 6.5 ISO, and you can follow the ESXi installation process.

2. In Oracle VirtualBox:

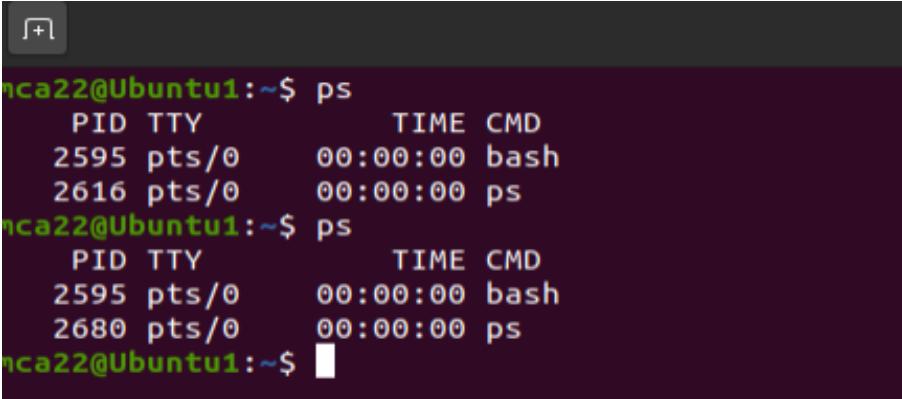
- a. Open Oracle VirtualBox and click "File" > "New" to create a new virtual machine.
- b. Configure the virtual machine settings, giving it a name, specifying the type as "Linux" and version as "Other Linux (64-bit)."
- c. Allocate sufficient CPU cores, memory, and storage to the virtual machine.
- d. After creating the VM, before starting it, click on "Settings."
- e. In the "Storage" section, add a new IDE controller and attach the ESXi 6.5 ISO to it.
- f. Start the virtual machine. It should boot from the ISO, allowing you to install ESXi.

Keep in mind that running ESXi as a nested virtualization environment may have limitations, and performance may not be the same as running it on physical hardware. Nested virtualization is primarily used for testing and learning purposes. For production use, ESXi should be installed on physical hardware.





```
sandeep@sandeep-VirtualBox:~$ mkdir Another
sandeep@sandeep-VirtualBox:~$ cd Another
sandeep@sandeep-VirtualBox:~/Another$ mkdir Dir
sandeep@sandeep-VirtualBox:~/Another$ cd Dir
sandeep@sandeep-VirtualBox:~/Another/Dir$ cd
sandeep@sandeep-VirtualBox:~/Another$ pwd
/home/sandeep
sandeep@sandeep-VirtualBox:~$ █
```



```
nca22@Ubuntu1:~$ ps
  PID TTY          TIME CMD
 2595 pts/0    00:00:00 bash
 2616 pts/0    00:00:00 ps
nca22@Ubuntu1:~$ ps
  PID TTY          TIME CMD
 2595 pts/0    00:00:00 bash
 2680 pts/0    00:00:00 ps
nca22@Ubuntu1:~$ █
```

P2.2:- Install multiple guest OS like Ubuntu Server, CentOS, Fedora etc. and manage the guest OS.

Solution:-

To install and manage multiple guest operating systems like Ubuntu Server, CentOS, Fedora, etc., you can use a virtualization platform such as VirtualBox or VMware. In this guide, I'll walk you through the process using VirtualBox as it's a free and widely used virtualization software.

Here are the steps to install and manage multiple guest OS on VirtualBox:

1. Download and Install VirtualBox:

- Go to the VirtualBox website (<https://www.virtualbox.org/>) and download the installer for your host operating system (e.g., Windows, macOS, or Linux).
- Install VirtualBox by following the on-screen instructions.

2. Download Guest OS ISO Images:

- Download ISO images of the guest operating systems you want to install. For example, download the ISO images for Ubuntu Server, CentOS, Fedora, etc. You can usually find these on the respective OS's official websites.

3. Create Virtual Machines (VMs):

- Open VirtualBox and click on "New" to create a new virtual machine.
- Follow the wizard to set up your virtual machine. You'll need to specify the name, type, and version of the guest OS (e.g., Ubuntu, Linux, Ubuntu (64-bit)).
- Allocate memory (RAM) to the virtual machine.
- Create a virtual hard disk (VDI, VHD, or VMDK) and specify its size.
- Configure the VM's settings as needed (e.g., processor cores, display settings, and network).

4. Install the Guest Operating System:

- Select the VM you just created in the VirtualBox Manager.
- Click on the "Start" button.
- VirtualBox will prompt you to select a startup disk. Choose the ISO image you downloaded for the guest OS.
- Follow the guest OS installation process. This will vary depending on the OS you're installing.

5. Repeat for Each Guest OS:

- Repeat the process for each guest operating system you want to install.

6. Manage Guest OS:

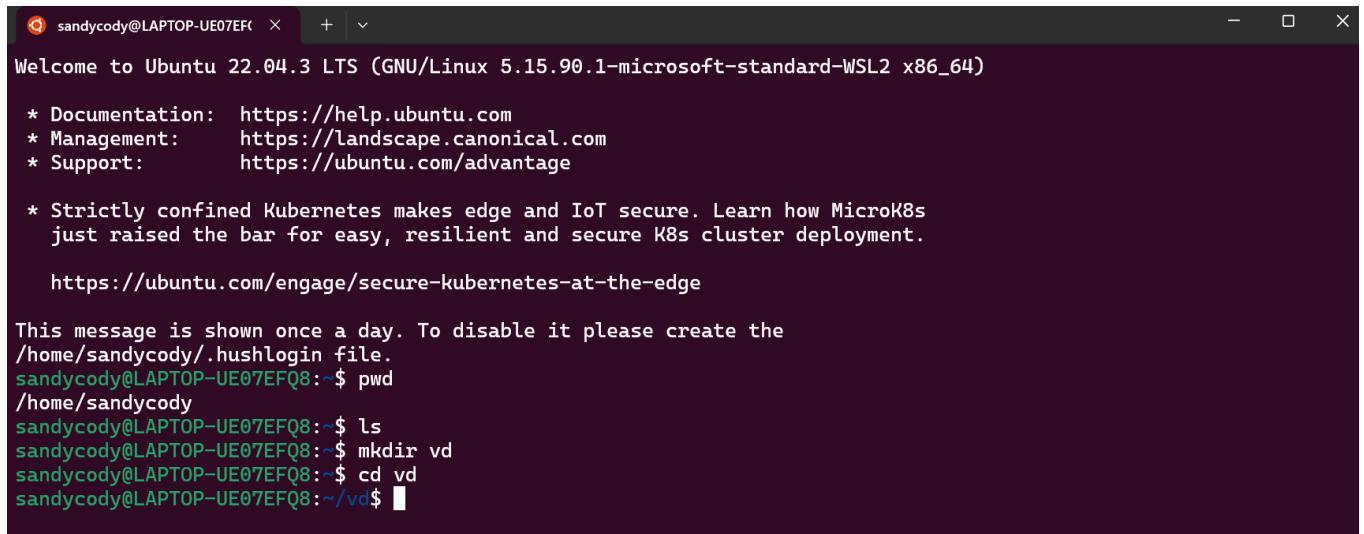
- Once your guest OS is installed, you can manage it through the VirtualBox Manager.

- You can start, pause, reset, and power off VMs from the Manager.
- You can also configure settings, such as network adapters and shared folders, for each VM.
- VirtualBox provides a way to access the VM's console for interaction with the guest OS.

7. Optional: Install Guest Additions:

- VirtualBox provides "Guest Additions" for improved performance and integration between the host and guest OS. Install Guest Additions within your guest OS after the initial setup.

Remember to consult the official documentation for VirtualBox and the specific guest OS you're working with for more detailed guidance on installation and configuration. This is a high-level overview to get you started with managing multiple guest OS on a single host using VirtualBox.



The screenshot shows a terminal window with the following content:

```
sandycody@LAPTOP-UE07EFQ8 ~ + - x
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.90.1-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
 just raised the bar for easy, resilient and secure K8s cluster deployment.

 https://ubuntu.com/engage/secure-kubernetes-at-the-edge

This message is shown once a day. To disable it please create the
/home/sandycody/.hushlogin file.
sandycody@LAPTOP-UE07EFQ8:~$ pwd
/home/sandycody
sandycody@LAPTOP-UE07EFQ8:~$ ls
sandycody@LAPTOP-UE07EFQ8:~$ mkdir vd
sandycody@LAPTOP-UE07EFQ8:~$ cd vd
sandycody@LAPTOP-UE07EFQ8:~/vd$ █
```

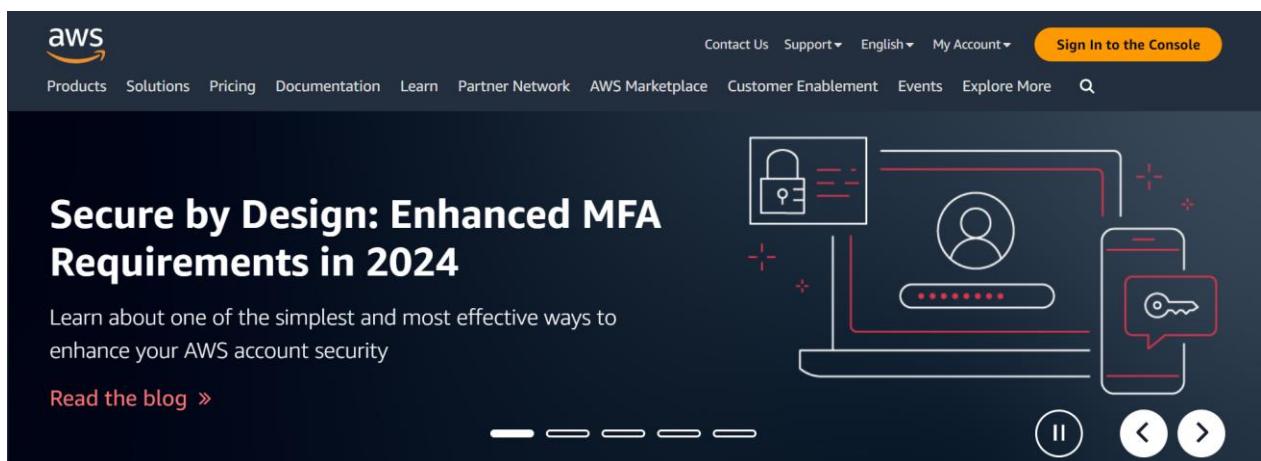
P3.1:- Find a procedure to set up an account with AWS, services it offers. Support your procedure with screenshots.

Solution:-

Procedure to Set Up an AWS Account:-

1. Visit the AWS Website:

Open your web browser and go to the AWS website at <https://aws.amazon.com/>.



2. Click on "Create an AWS Account":

On the AWS homepage, click on the "Create an AWS Account" button, usually found in the top right corner.

The image shows the AWS sign-in interface on the left and a promotional card for 'AWS Skill Builder for Teams' on the right.

AWS Sign-in:

- Root user:** Selected radio button. Description: Account owner that performs tasks requiring unrestricted access. [Learn more](#).
- IAM user:** Unselected radio button. Description: User within an account that performs daily tasks. [Learn more](#).

Root user email address:

Next button.

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

New to AWS? [Create a new AWS account](#)

AWS Skill Builder for Teams:

UNLOCK INNOVATION

AWS Skill Builder for Teams

Build expertise to reduce costs, become more agile, and innovate faster

[Learn more >](#)

3. Choose Your Account Type:

You'll be presented with two options: "Root user" and "IAM user." Select "Root user" to create an AWS account.

The image shows the AWS sign-in interface on the left and a promotional card for 'AWS Skill Builder for Teams' on the right.

AWS Sign-in:

- Root user:** Selected radio button. Description: Account owner that performs tasks requiring unrestricted access. [Learn more](#).
- IAM user:** Unselected radio button. Description: User within an account that performs daily tasks. [Learn more](#).

Root user email address:

Next button.

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

New to AWS? [Create a new AWS account](#)

AWS Skill Builder for Teams:

UNLOCK INNOVATION

AWS Skill Builder for Teams

Build expertise to reduce costs, become more agile, and innovate faster

[Learn more >](#)

4. Provide Your Email Address:

Enter your email address, choose a password, and click "Next."



Root user sign in [?](#)

Email: mca22.sandeepwadhawan@bvicam.in

Password

[Forgot password?](#)

.....

[Sign in](#)

[Sign in to a different account](#)

[Create a new AWS account](#)

UNLOCK INNOVATION

AWS Skill Builder for Teams

Build expertise to
reduce costs,
become more agile,
and innovate faster

[Learn more >](#)



5. Enter Your Account Information:

Fill out the required account information, including your name, company name, phone number, and address. Click "Next" when you're finished.



Sign up for AWS

Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.



Always free

Never expires



12 months free

Start from initial sign-up date



Trials

Start from service activation date

Contact Information

How do you plan to use AWS?

- Business - for your work, school, or organization
 Personal - for your own projects

Who should we contact about this account?

Full Name

Phone Number

+1 222-333-4444

Country or Region

United States

Address

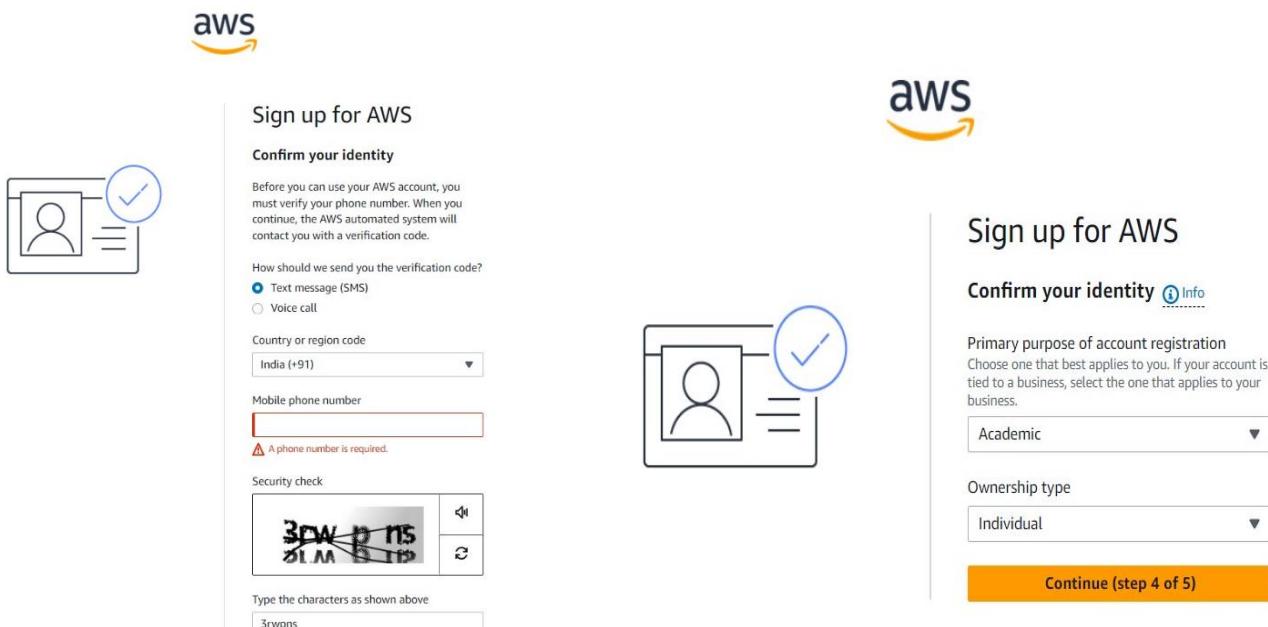
Apartment, suite, unit, building, floor, etc.

City

6. Contact Information and Identity Verification:

Enter your contact information and complete the identity verification process. You

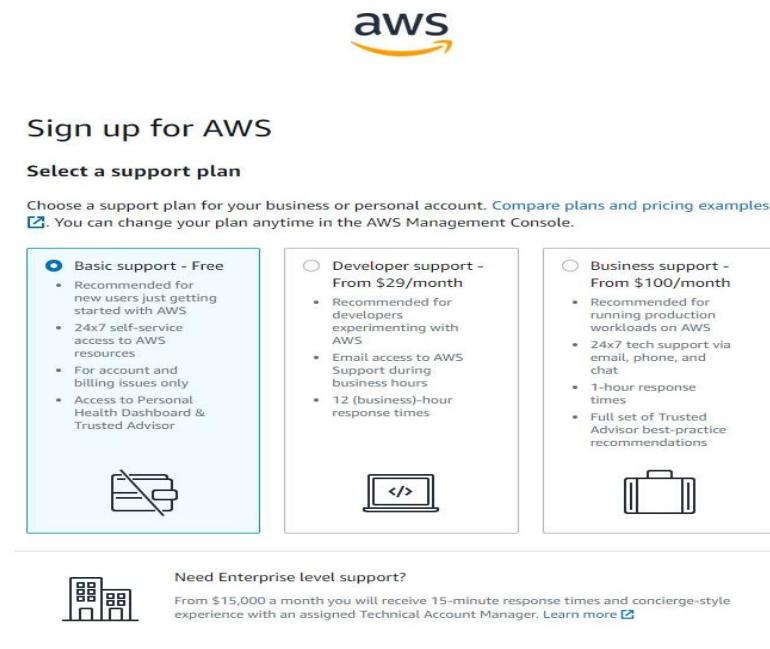
may be required to provide a phone number for verification.



The image shows two screenshots of the AWS sign-up process. The left screenshot shows the 'Sign up for AWS' page with a 'Confirm your identity' section. It includes a placeholder for a profile picture with a checkmark, a dropdown for country/region set to 'India (+91)', and a mobile phone number input field with an error message 'A phone number is required.' Below is a 'Security check' section with a CAPTCHA image showing '3rwPns' and a text input field where '3rwPns' is typed. The right screenshot shows a similar 'Sign up for AWS' page with a 'Confirm your identity' section. It includes a placeholder for a profile picture with a checkmark, a dropdown for 'Primary purpose of account registration' set to 'Academic', and a dropdown for 'Ownership type' set to 'Individual'. A large orange 'Continue (step 4 of 5)' button is at the bottom.

7. Choose a Support Plan:

AWS offers a free support plan, and you can choose to subscribe to a paid plan if you wish. Select the appropriate option and click "Continue."



The image shows the 'Sign up for AWS' page with the 'Select a support plan' section. It features three options: 'Basic support - Free' (selected), 'Developer support - From \$29/month', and 'Business support - From \$100/month'. Each option has a detailed description and an icon. Below the plans is a section for 'Enterprise level support' with a building icon and a note about \$15,000 per month. At the bottom is an orange 'Complete sign up' button.

8. Payment Information:

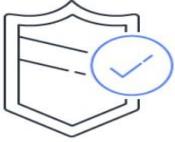
Sandeep Wadhawan (01411604422)

Enter your payment information, including credit card details. AWS uses this information for billing purposes. Click "Verify and Add" to confirm your credit card.

aws

Secure verification

We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to \$1 USD (or an equivalent amount in local currency) as a pending transaction for 3-5 days to verify your identity.



Sign up for AWS

Billing Information

Credit or Debit card number

VISA AMEX RuPay

AWS accepts all major credit and debit cards. To learn more about payment options, review our FAQ

Expiration date

November 2026

Security code

Cardholder's name

Sandeep Wadhawan

Billing address

Use my contact address
2105/4F Prem Nagar, New Delhi - 110008
New Delhi Delhi 110008
IN

Use a new address

9. Mobile Phone Verification:

AWS may send a verification code to your mobile phone. Enter the code to verify your identity.

aws



Sign up for AWS

Confirm your identity

Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.

How should we send you the verification code?

Text message (SMS)
 Voice call

Country or region code

India (+91)

Mobile phone number

⚠ A phone number is required.

Security check



Type the characters as shown above

3rwpns

10. Accept the AWS Customer Agreement:

Review the AWS Customer Agreement and click "Create Account and Continue."

11. Wait for AWS Account Activation:

Your AWS account will be reviewed and activated. This may take a short amount of time.



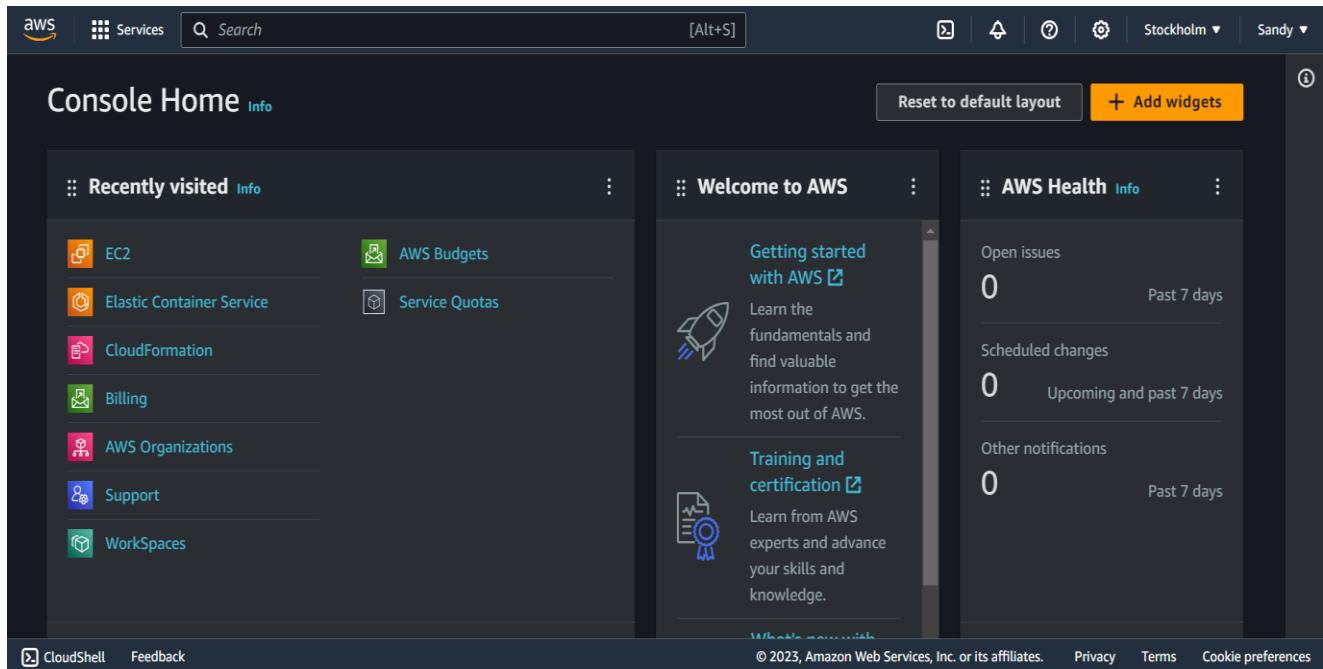
12. Set Up Multi-Factor Authentication (MFA):

After your account is activated, it's recommended to set up Multi-Factor Authentication (MFA) for added security. This can be done from the AWS Management Console.



13. Access AWS Services:

Once your account is set up and activated, you can access the AWS Management Console, where you can explore and use various AWS services.



P3.2:- Demonstrate the steps with screenshots to add a new instance and create a virtual machine in Amazon Web Service using EC2.

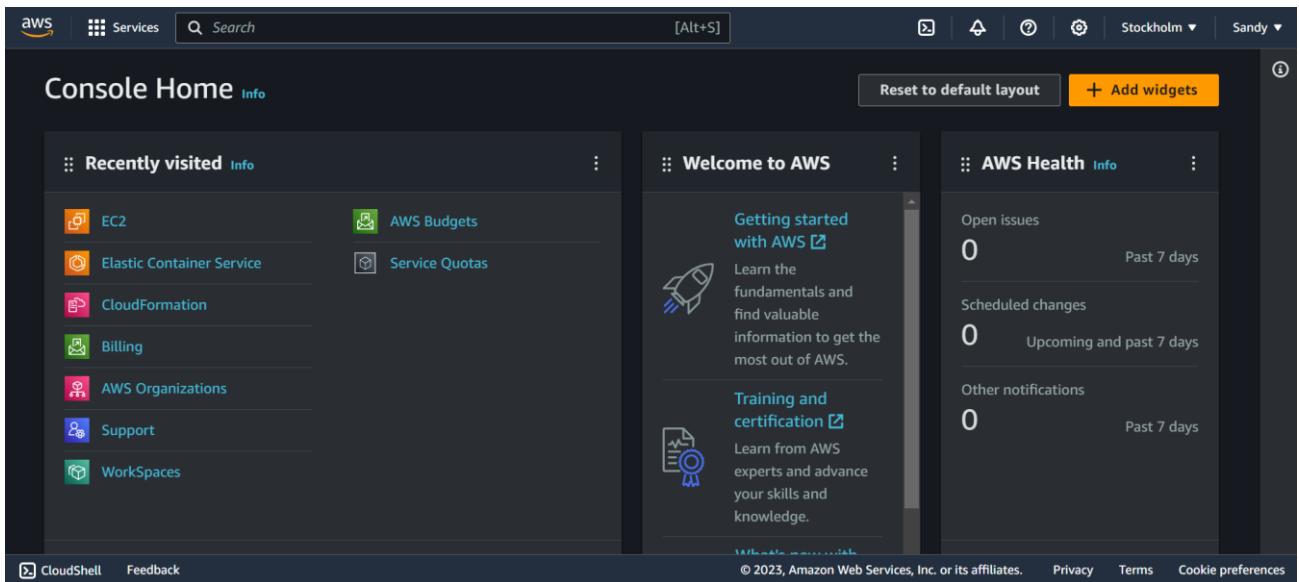
Solution:-

We can follow these steps in the AWS Management Console:

Step 1: Sign in to AWS

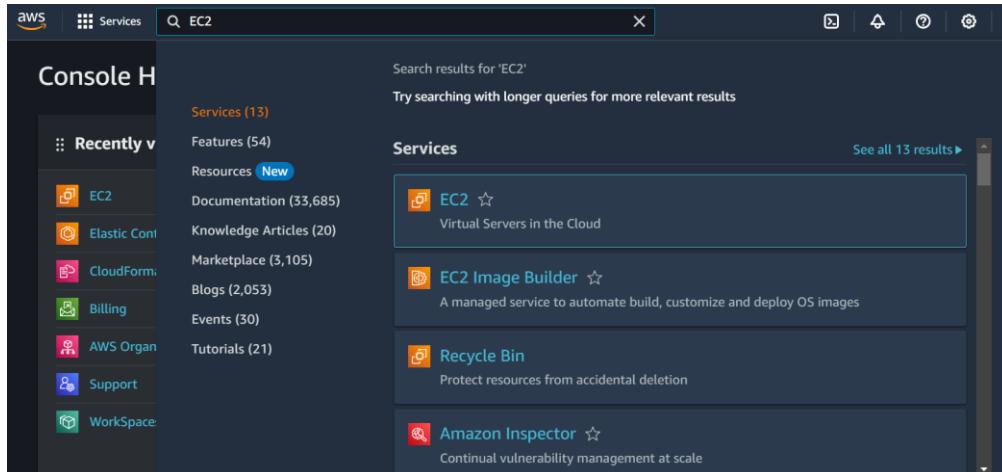
Go to the AWS Management Console (<https://aws.amazon.com/console/>). Sign in with your AWS account credentials.

Cloud Computing



Step 2: Access the EC2 Dashboard

Once you're logged in, you'll be on the AWS Management Console dashboard. In the "Find Services" search bar, type "EC2" and select "EC2" from the search results.



Step 3: Launch an Instance

In the EC2 Dashboard, click the "Launch Instance" button.

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with navigation links like 'EC2 Global View', 'Events', 'Instances' (with sub-links for 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', and 'Capacity Reservations'), and 'Images' (with sub-links for 'AMIs' and 'AMI Catalog'). The main area has a grid of metrics: 'Instances (running)' 0, 'Auto Scaling Groups' 0, 'Dedicated Hosts' 0, 'Elastic IPs' 0, 'Instances' 0, 'Key pairs' 1, 'Load balancers' 0, 'Placement groups' 0, 'Security groups' 3, 'Snapshots' 0, and 'Volumes' 0. Below this is a 'Launch instance' section with a large orange 'Launch instance' button and a 'Migrate a server' link. To the right is a 'Service health' section with a 'AWS Health Dashboard' link and a status indicator.

Step 4: Choose an Amazon Machine Image (AMI)

In the "Choose an Amazon Machine Image (AMI)" step, you can select the base operating system for your instance. You can choose from various AMIs, including Amazon Linux, Ubuntu, Windows, and more.

After selecting an AMI, click "Next: Configure Instance Details."

The screenshot shows the 'Launch an instance' wizard. The breadcrumb navigation shows 'EC2 > Instances > Launch an instance'. The main title is 'Launch an instance' with an 'Info' link. A descriptive text says '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.' Below this is a 'Name and tags' section with an 'Info' link. It has a 'Name' input field containing 'Instance1' and a 'Add additional tags' link.

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

Quick Start

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base Free tier eligible ▾
ami-009b52c0f357dd769 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

Architecture 64-bit (x86) **AMI ID** ami-009b52c0f357dd769 **Verified provider**

Step 5: Configure Instance Details

In this step, you can configure various instance details such as the number of instances, network settings, and IAM roles.

Customize your instance configuration according to your requirements and click "Next: Add Storage."

Instance type Info

t3.micro Free tier eligible

Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.0708 USD per Hour
On-Demand SUSE base pricing: 0.0108 USD per Hour
On-Demand Linux base pricing: 0.0108 USD per Hour
On-Demand Windows base pricing: 0.02 USD per Hour

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

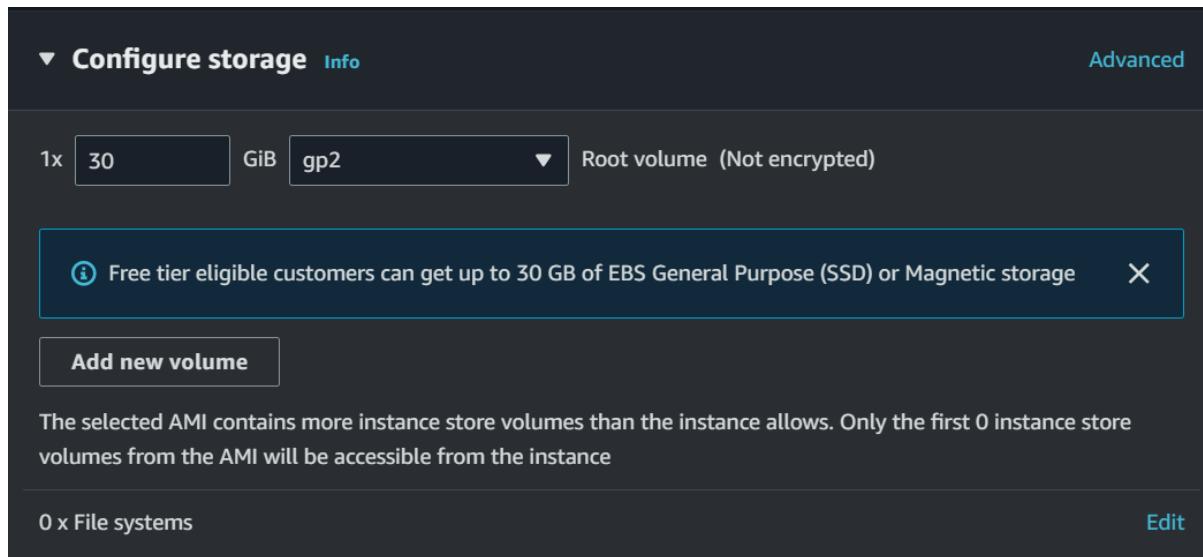
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required sandyKey Create new key pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

Step 6: Add Storage

In the "Add Storage" step, you can specify the storage volume for your instance. You can change the volume size, type, and add additional volumes if needed. Adjust the storage settings as required and click "Next: Add Tags."



Step 7: Add Tags (Optional)

You can add tags to your instance to help organize and identify it. Tags are key-value pairs that you can use for tracking and categorization.

Add tags if necessary, and then click "Next: Configure Security Group."

Step 8: Configure Security Group

In the "Configure Security Group" step, you define the rules that control inbound and outbound traffic to your instance.

Create a new security group or select an existing one. Ensure that you allow the necessary ports and protocols for your application.

Click "Review and Launch" when you're ready.

Network [Info](#)
vpc-012951894c0a7787c

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-3' with the following rules:

<input checked="" type="checkbox"/> Allow RDP traffic from Helps you connect to your instance	Anywhere 0.0.0.0/0
<input type="checkbox"/> Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server	
<input type="checkbox"/> 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. **X**

Step 9: Review and Launch

Review your instance settings to make sure everything is correct. Click "Launch" to start the instance creation process.

Review commands

The following API calls will be used to launch your instance.

Instance setup

API call: RunInstances

The following input will be used in the SDK RunInstances request. [Learn more](#)

Any new security groups created by the security group requests in the sections below will be added to this input at launch time.

```
{
  "MaxCount": 1,
  "MinCount": 1,
  "ImageId": "ami-009b52c0f357dd769",
  "InstanceType": "t3.micro",
  "KeyName": "sandyKey",
  "EbsOptimized": true,
  "NetworkInterfaces": [
    {
      "SubnetId": "subnet-00000000000000000000000000000000"
    }
  ]
}
```

Copy

Close

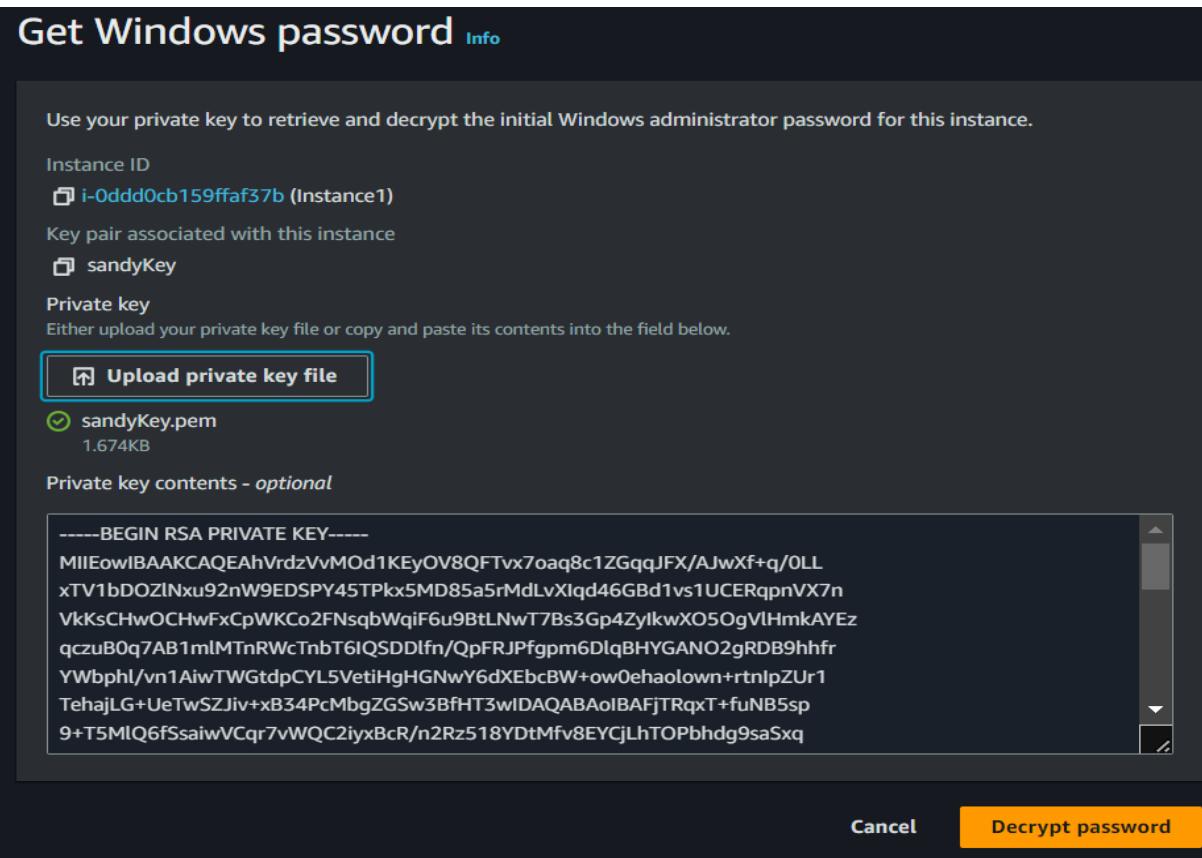
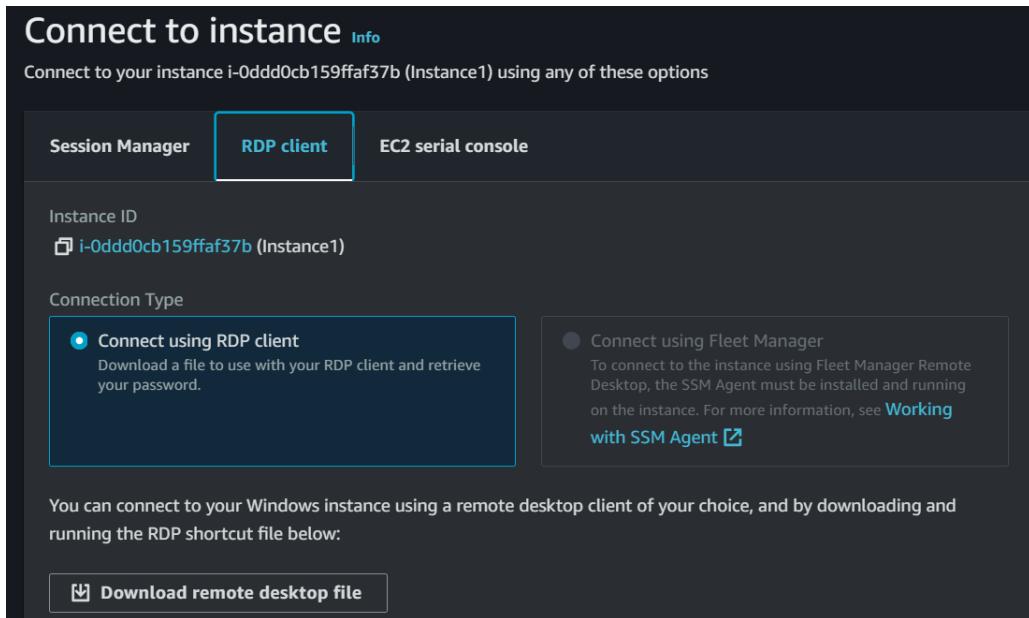
EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0ddd0cb159ffaf37b)

▶ Launch log

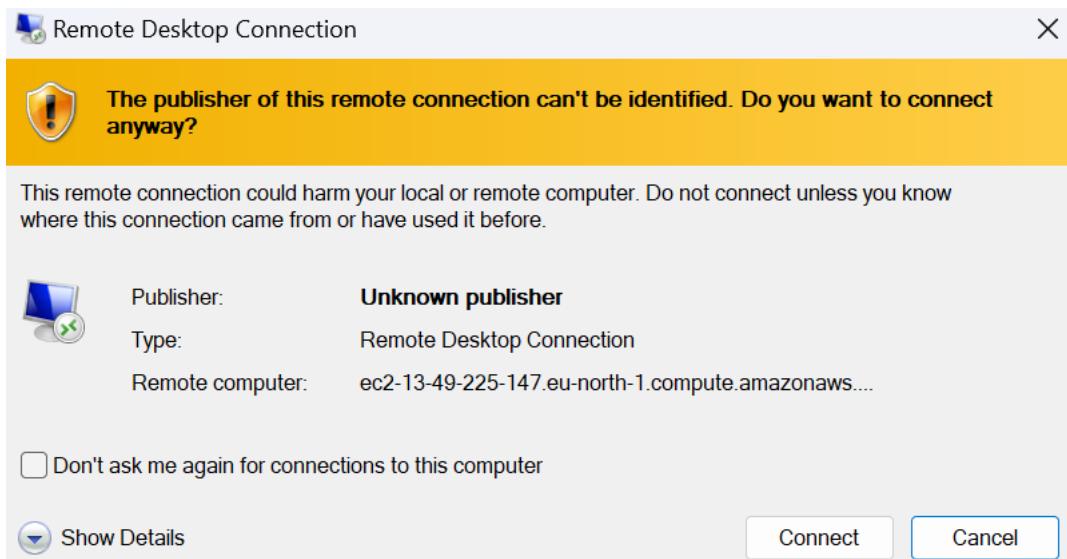
Step 10: Choose an Existing Key Pair or Create a New One

If you already have an SSH key pair, select it. If not, you can create a new key pair. To create a new key pair, enter a name and download the private key file (.pem). Make sure to keep this private key safe as you'll need it to access your instance.



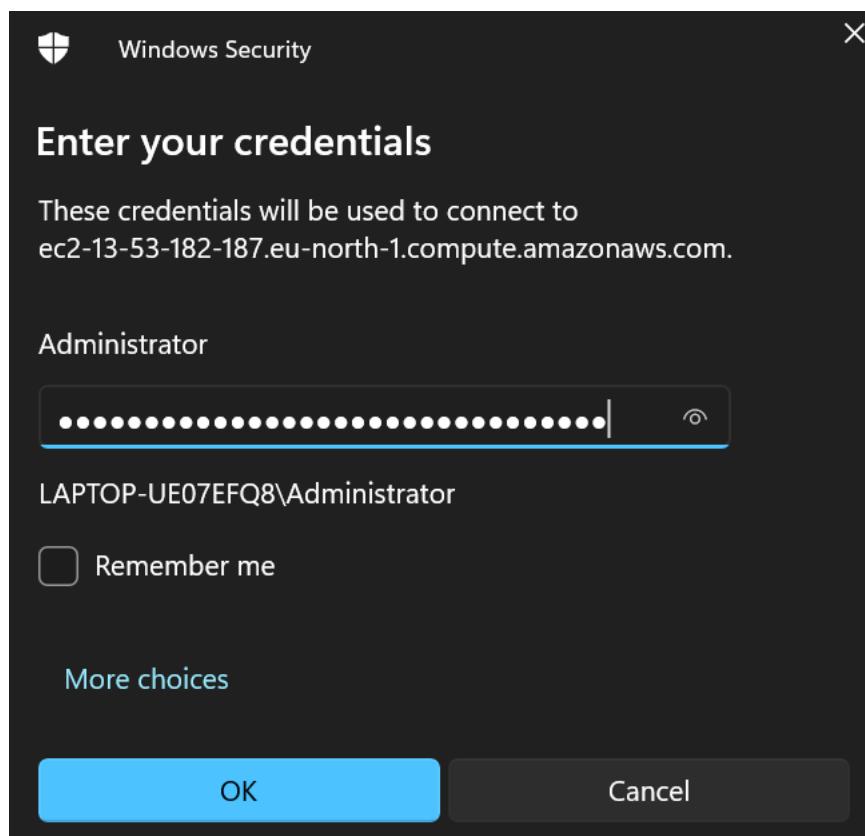
Step 11: Open RDP shortcut file

Click on connect option after opening the downloaded RDP file.



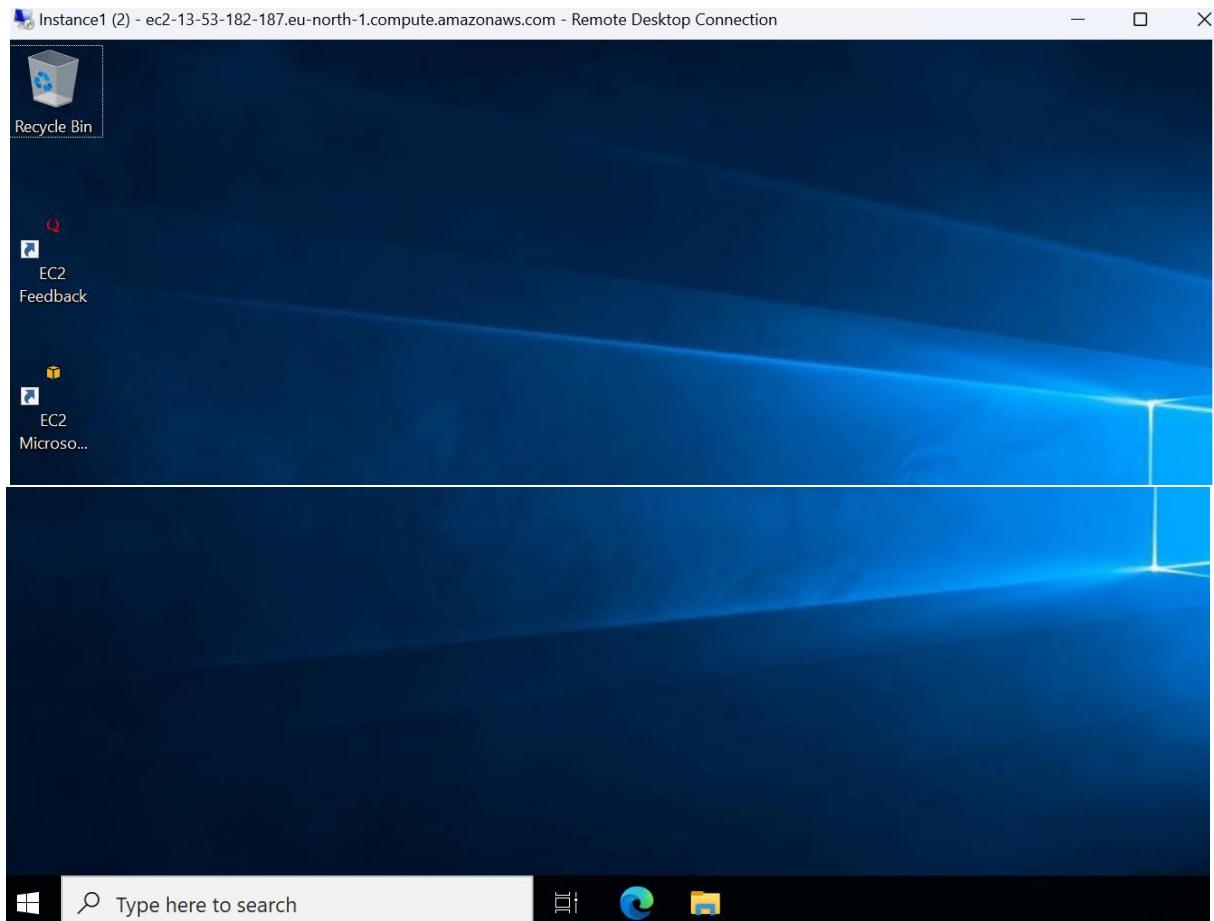
Step 12: Enter your credentials

Paste the decrypted password in the password column and click "OK".



Step 13: Launching of Virtual Machine

Finally the Virtual Machine will be launched on your Operating System.



Problem 4:- Suppose you are an AWS cloud consultant. Mr. Hemant came to you with following constraints:

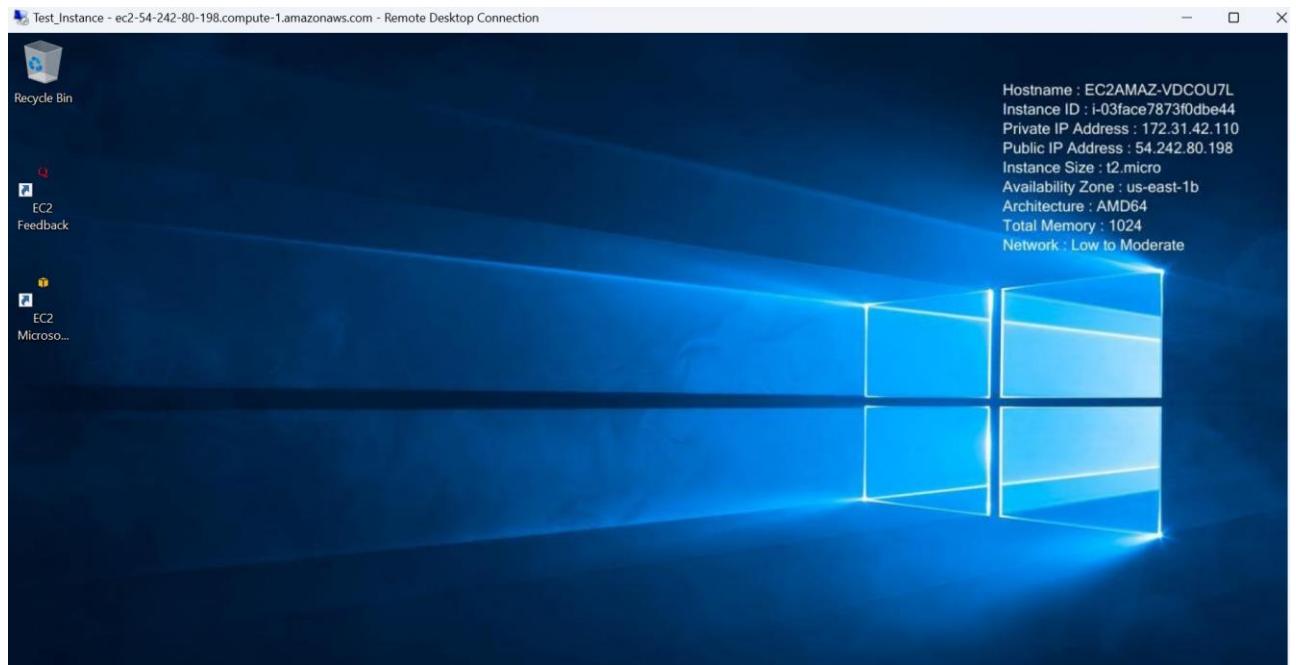
- 1. He needs a remote desktop Login of the virtual machine you created using EC2 instance.**
- 2. Need to create a webpage using Webserver IIS to demonstrate the importance of cloud.**

Solution:-

Creating a basic web server on an EC2 instance running Windows with IIS (Internet Information Services) installed is relatively straightforward. Here are the steps to set up a simple web server:

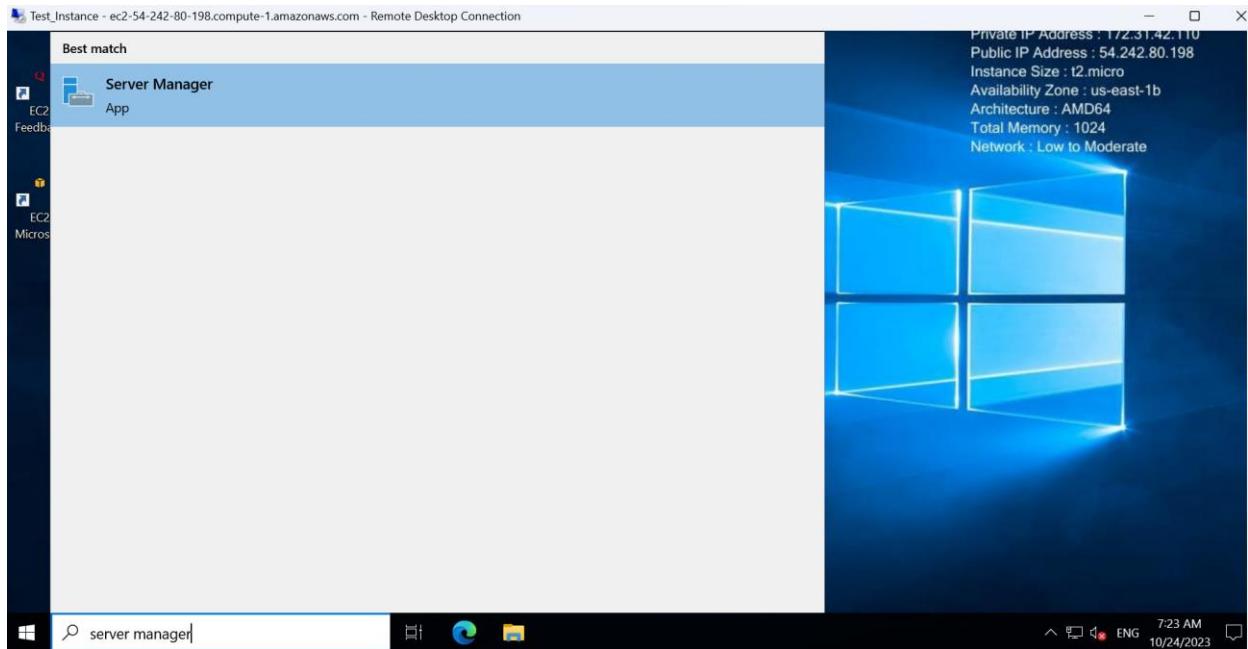
1. Connect to Your EC2 Instance:

- Access your Windows EC2 instance using Remote Desktop Protocol (RDP). We should have already created this instance as per Mr. Hemant's requirements.



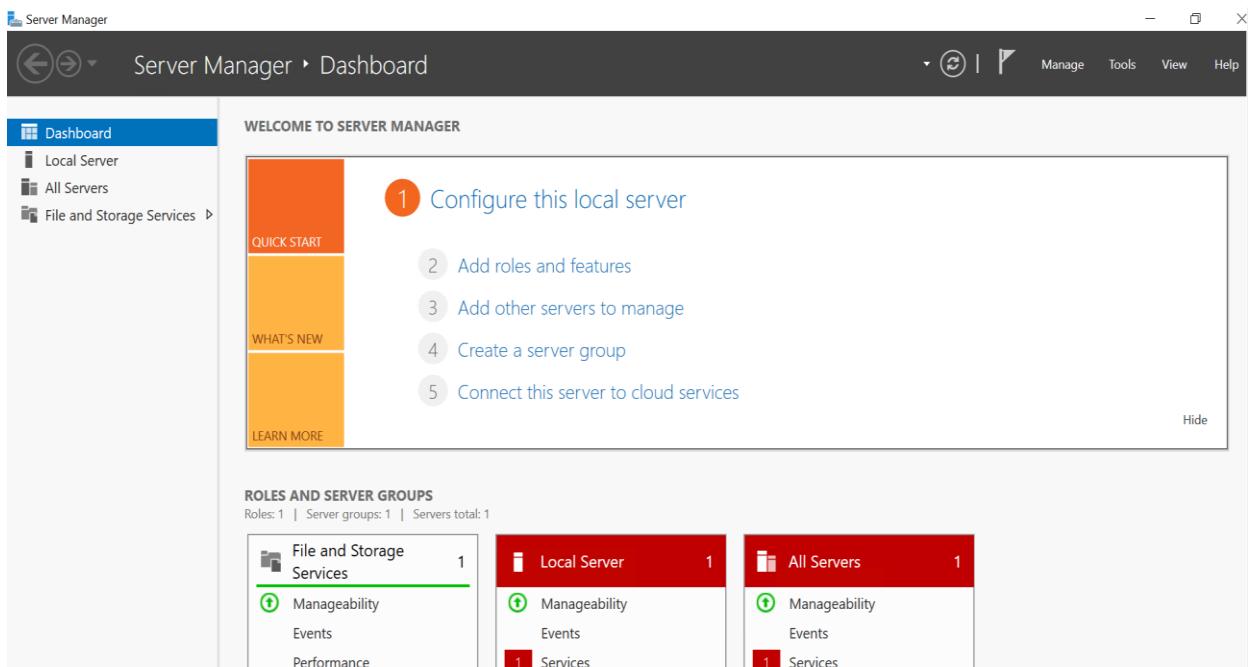
2. Access Internet Information Services (IIS):

- Once you're logged into your EC2 instance, open the "Server Manager" from the Windows Start menu.

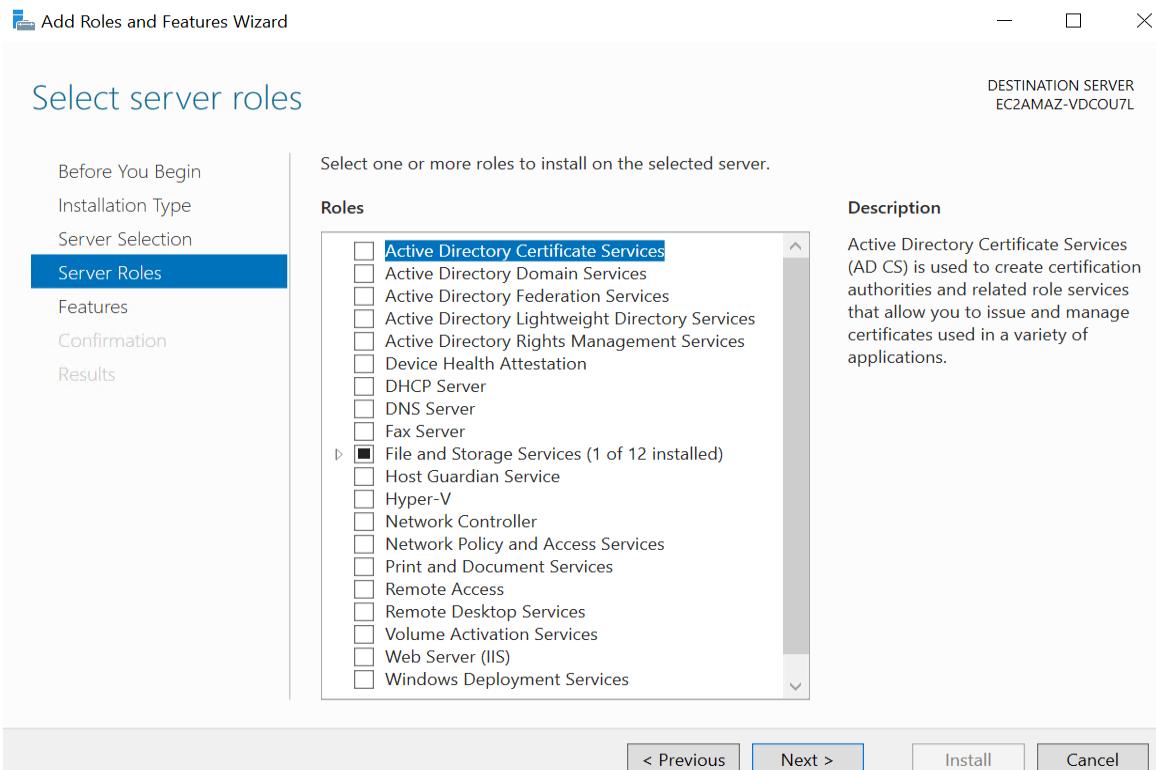


3. Install IIS:

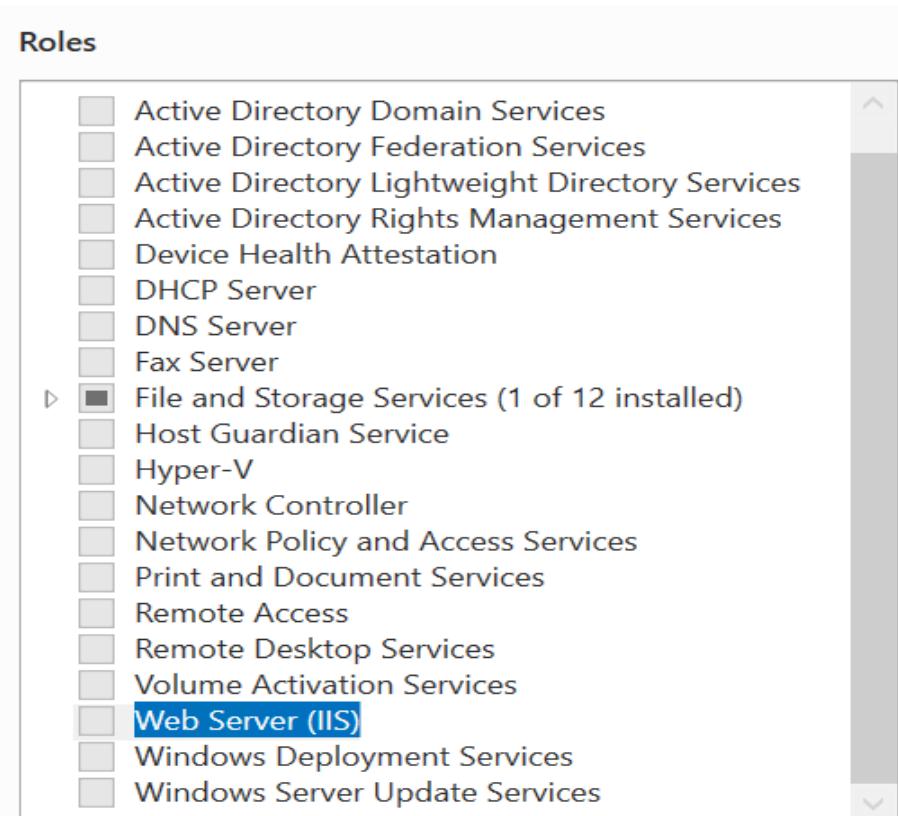
- In the "Server Manager," click on "Add roles and features."



- Select "Role-based or feature-based installation" and click "Next."

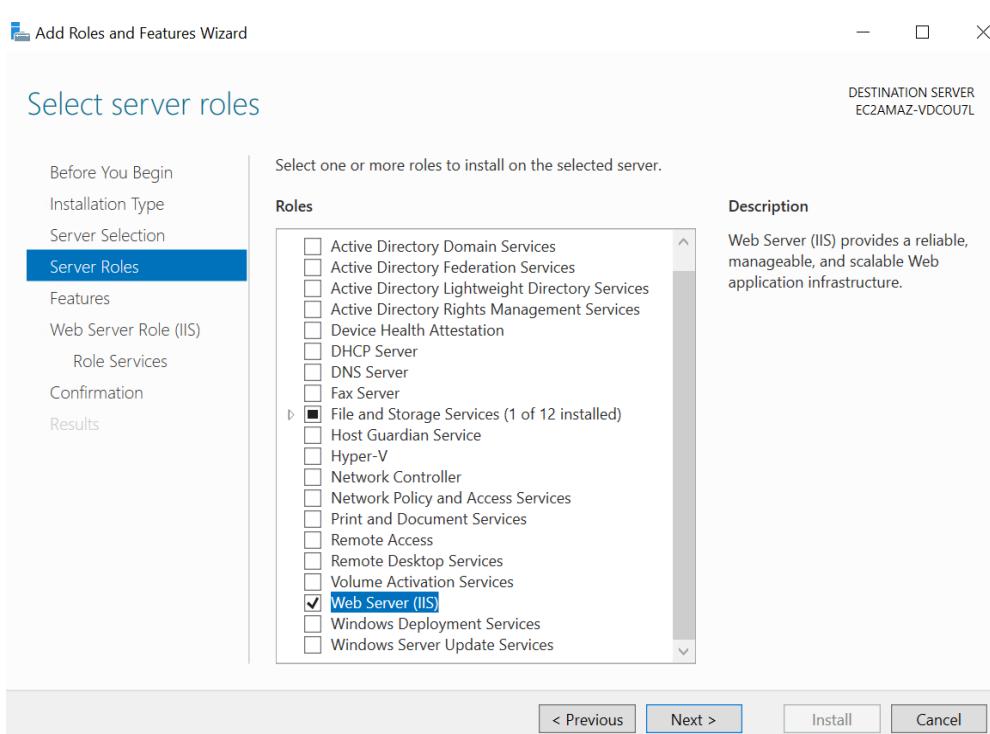
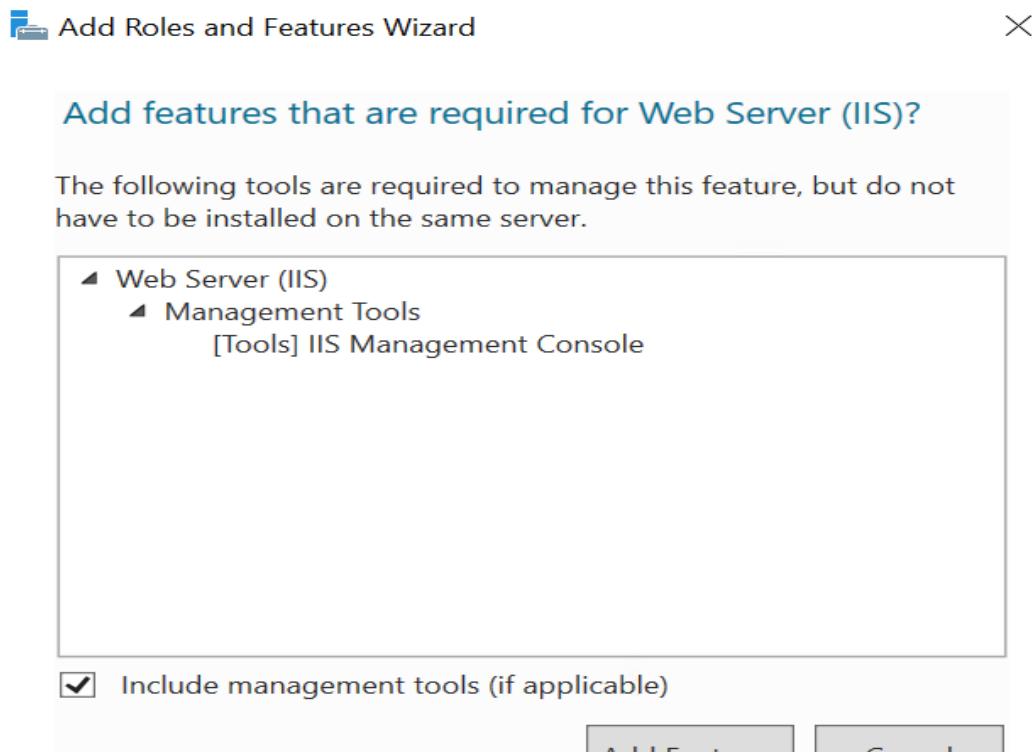


- In the "Select features" section, scroll down and select "Web Server (IIS)."

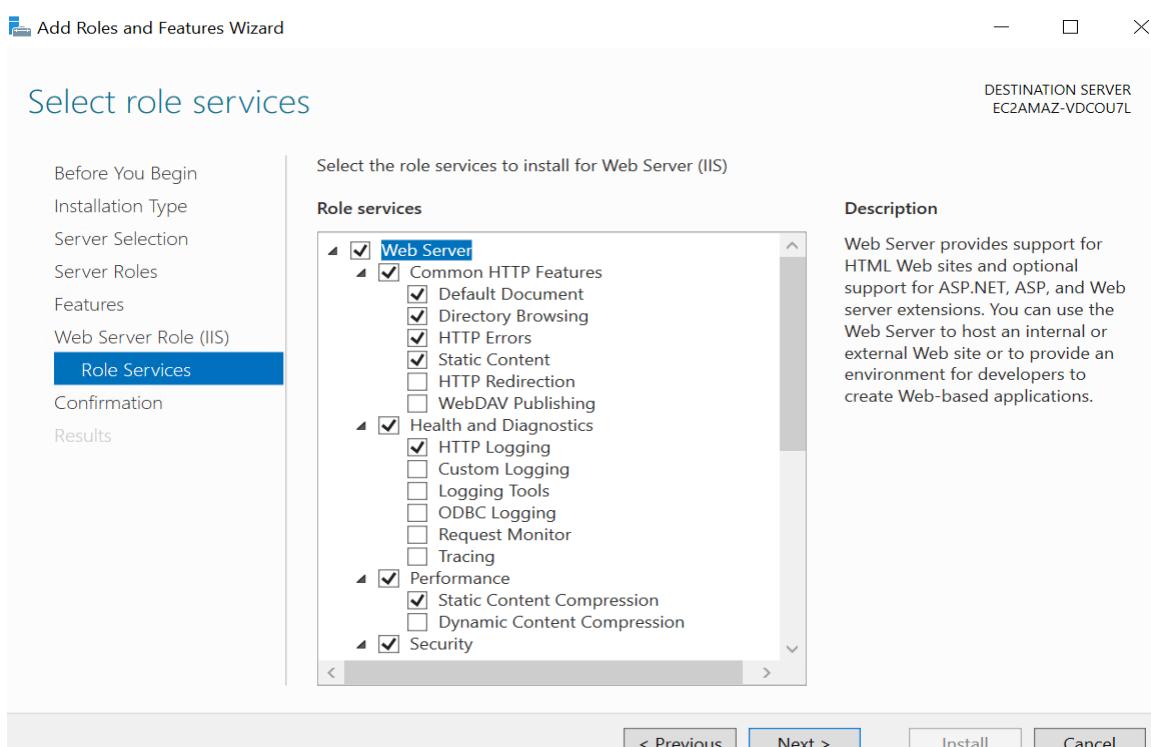
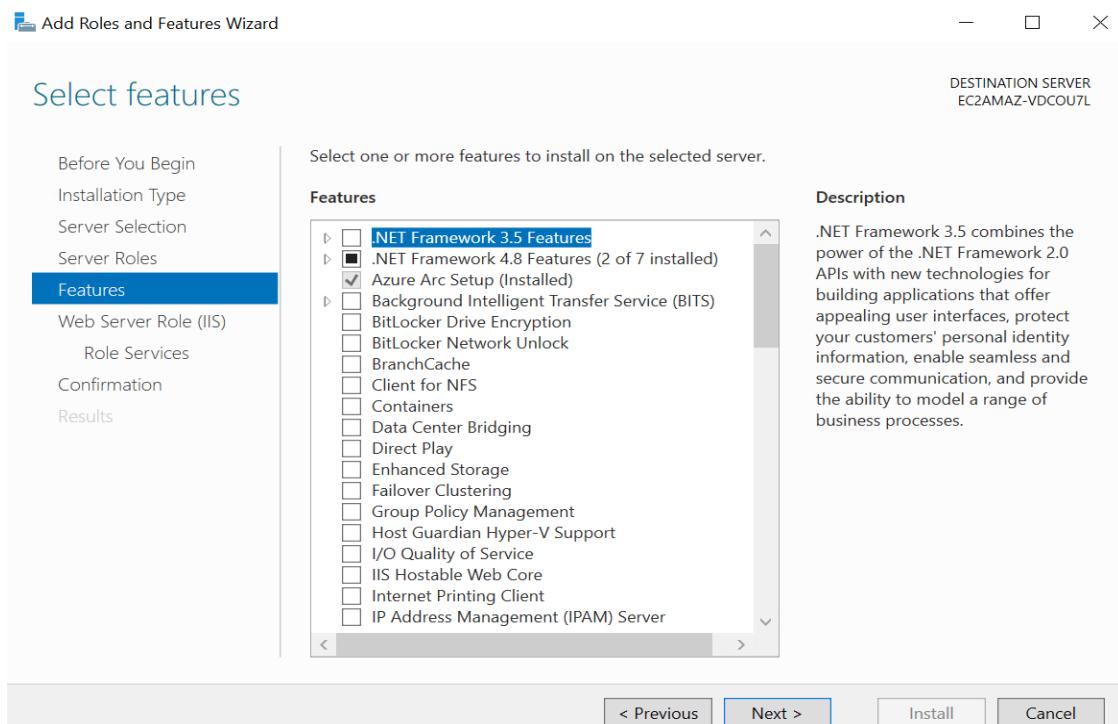


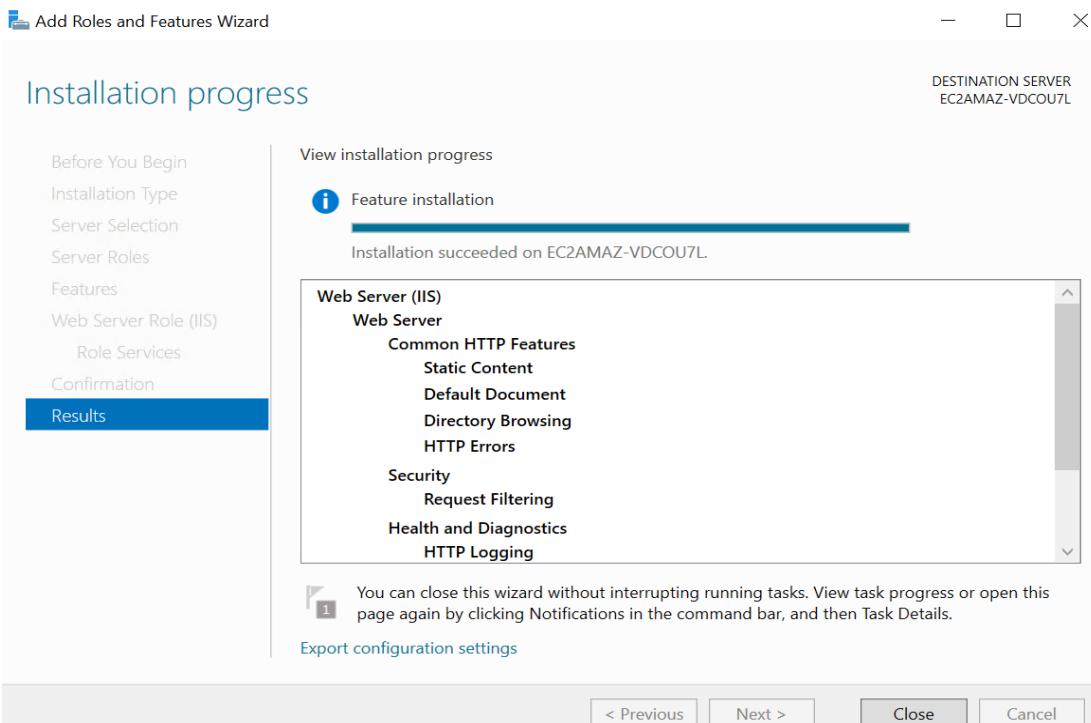
- Click "Next" to add the required features, then click "Install" to start the installation process.

Cloud Computing



Cloud Computing





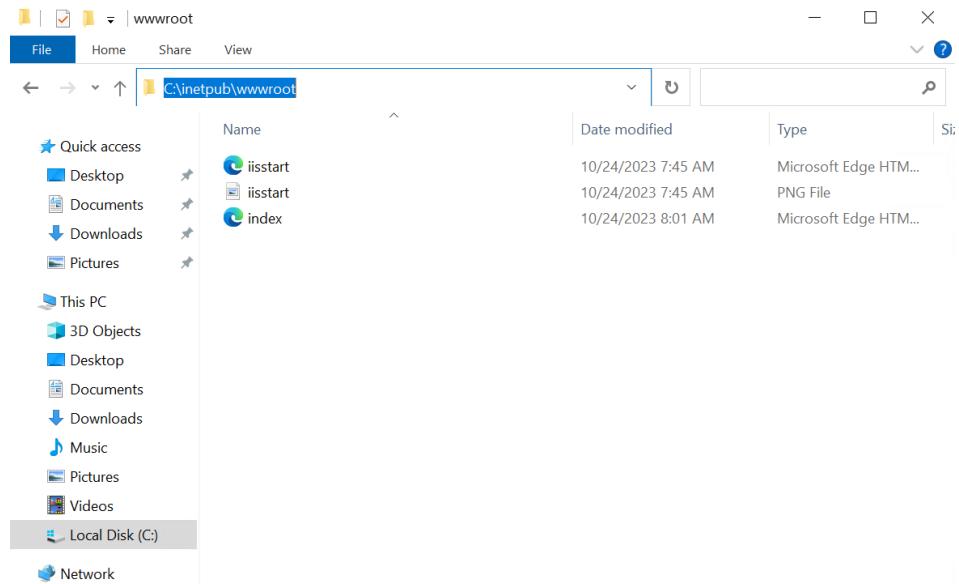
4. Create a Simple Web Page:

- After IIS is installed, you can create a basic HTML webpage to demonstrate the importance of the cloud. You can use any text editor, such as Notepad, to create an HTML file.

```
<html>
  <head>
    <title> Creation of Webpage </title>
  </head>
  <body>
    <h1> Welcome to Website using IIS </h1>
    <div> This is the basic div tag </div>
  </body>
</html>
```

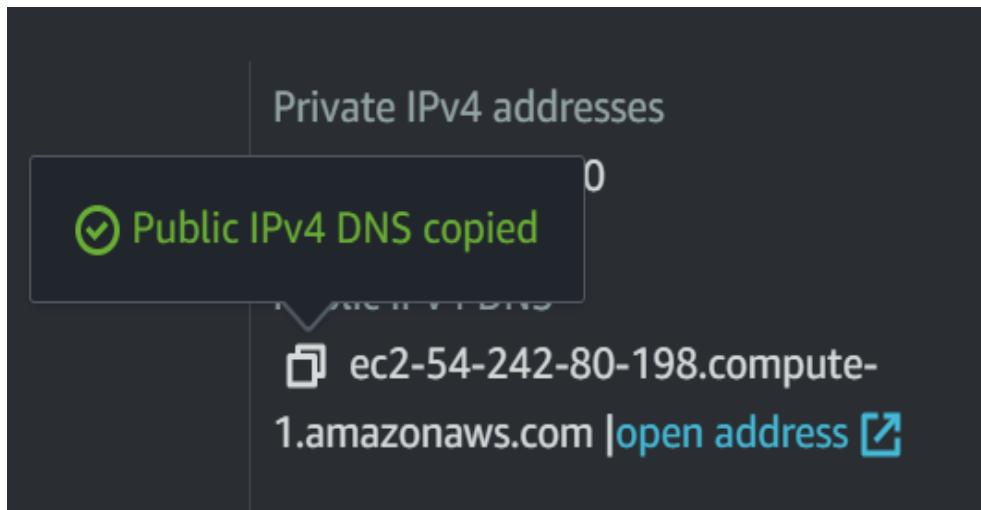
- Save the HTML file in the default root directory for IIS, which is typically "C:\inetpub\wwwroot\". You can give it a name like "index.html".

Cloud Computing

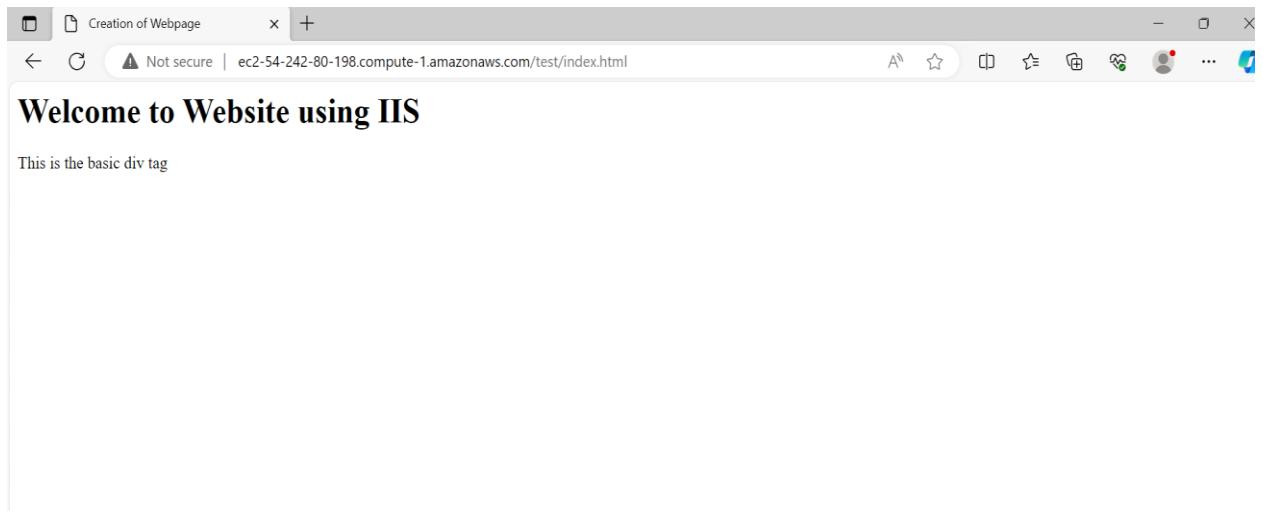


5. Test the Web Page:

- Open a web browser on your local machine and enter the public IP address or DNS name of your EC2 instance in the address bar.



- You should be able to access the HTML page you created. The URL would be something like: `http://<Your-EC2-Public-IP>/index.html`.



Please note that this is a basic setup to demonstrate the functionality of a web server in a cloud environment. In a production environment, you would want to take additional steps for security, scalability, and performance optimization.

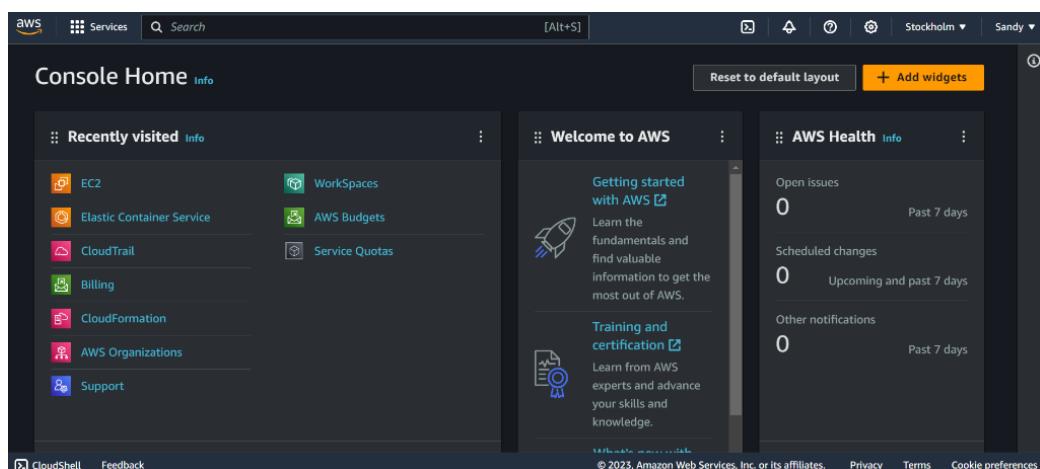
Problem 5:- Assume, you are technical advisor in your organization. The organization's vision is to provide use the cloud services in AWS. You are directed to give Roles, authentication and authorizations to employees using a particular service of cloud.

Solution:-

To provide roles, authentication, and authorizations to employees using AWS Identity and Access Management (IAM) service, follow these steps:

1. Create IAM Users:

- Log in to the AWS Management Console



- Open the IAM dashboard

User groups	Users	Roles	Policies	Identity providers
0	2	6	0	0

- Click on "Users" in the left navigation pane.

The screenshot shows the AWS IAM 'Users' page. At the top, there's a breadcrumb navigation 'IAM > Users'. Below it, a header says 'Users (2) Info' with buttons for 'Create user' and 'Delete'. A search bar and a page number '1' are also present. The main area is a table with columns: 'User name', 'Path', 'Groups', 'Last activity', 'MFA', and 'Pass'. Two users are listed: 'Sandeep' and 'sandy'. Both users have a green checkmark icon next to their names, indicating they have 2 and 8 factors respectively.

- Click "Create user" to create a new IAM user.

The screenshot shows the 'Specify user details' step of the IAM User creation wizard. It has a title 'User details'. Under 'User name', the value 'Devil' is entered. A note below says the user name can have up to 64 characters and lists valid characters: A-Z, a-z, 0-9, and + = . @ _ - (hyphen). There's an optional checkbox 'Provide user access to the AWS Management Console' which is unchecked. A note explains that if checked, it's a best practice to manage access in IAM Identity Center. A callout box provides information about generating programmatic access keys for AWS CodeCommit or Amazon Keyspaces after user creation. At the bottom are 'Cancel' and 'Next' buttons.

- Set the user's custom password

Cloud Computing

Are you providing console access to a person?

User type

Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keypairs, or a backup credential for emergency account access.

Console password

Autogenerated password
You can view the password after you create the user.

Custom password
Enter a custom password for the user.

• Must be at least 8 characters long
• Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | '

Show password

Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, you can generate them after you create this IAM user. [Learn more](#)

Cancel **Next**

- Configure the user's permissions (either add them to an existing group or attach policies directly).

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1132)
Choose one or more policies to attach to your new user.

Filter by Type
Q: AmazonEC2Full X All types 1 match

Policy name	Type	Attached entities
<input checked="" type="checkbox"/>  AmazonEC2FullAccess	AWS managed	2

▼ Set permissions boundary - optional

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Use a permissions boundary to control the maximum permissions
You can select one of the existing permissions policies to define the boundary.

Cancel Previous **Next**

- Complete the user creation process by reviewing all the details entered

Cloud Computing

User details

User name Devil	Console password type Custom password	Require password reset No
--------------------	--	------------------------------

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

⌚ User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

IAM > Users > Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Email sign-in instructions

Console sign-in URL
https://54727295667.sigin.aws.amazon.com/console

User name
Devil

Console password
***** Show

Cancel Download .csv file Return to users list

2. Define IAM Groups:

- IAM groups help you manage permissions for multiple users. Create different user groups based on job roles or responsibilities (e.g., administrators, developers).

Cloud Computing

The screenshot shows the AWS IAM User groups page. At the top, there is a header with the IAM logo and the text "User groups". Below the header, a title "User groups (0) Info" is displayed, followed by a sub-instruction: "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." A search bar labeled "Search" is present. To the right of the search bar are buttons for "Delete" and "Create group". Below the search bar is a table header with columns: "Group name", "Users", "Permissions", and "Creation time". The main content area displays the message "No resources to display".

The screenshot shows the "Name the group" step of the IAM User group creation wizard. It has two sections: "User group name" and "Add users to the group - Optional (1/3)". In the "User group name" section, the name "Administrator" is entered into a text input field. In the "Add users to the group" section, the user "Devil" is selected from a list of users: Devil, Sandeep, and sandy.

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+-=._@-' characters.

Add users to the group - Optional (1/3) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time
Devil	0	None	8 minutes ago
Sandeep	0	None	2 days ago
sandy	0	2 days ago	8 days ago

The screenshot shows the "Attach permissions policies" step of the IAM User group creation wizard. It has two sections: "Attach permissions policies - Optional (1/882)" and a table of attached policies. One policy, "AdministratorAccess", is selected and attached to the group.

Attach permissions policies - Optional (1/882) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Policy name	Type	Used as	Description
AdministratorAccess	AWS managed - job funct...	None	Provides full access to AWS services and resources.

3. Creating and Authorizing IAM Roles:

- IAM roles are used for granting temporary permissions to AWS services, applications, or other AWS accounts.

Cloud Computing

The screenshot shows the AWS IAM Roles page. At the top, there are buttons for 'Create role' (highlighted in orange) and 'Delete'. Below is a search bar and a table listing five roles:

Role name	Trusted entities	Last activity
AWSServiceRoleForECS	AWS Service: ecs (Service-Linked Role)	Yesterday
AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (S)	Yesterday
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
ecsTaskExecutionRole	AWS Service: ecs-tasks	Yesterday

- Click on “Create role” and select trusted entity type.

The screenshot shows the 'Select trusted entity' configuration page. It has two main sections: 'Trusted entity type' and 'Use case'.

Trusted entity type:

- AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case:

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case:

EC2

Choose a use case for the specified service.

Use case

EC2
Allows EC2 instances to call AWS services on your behalf.

- Assign “AmazonEC2FullAccess” policy to the role.

The screenshot shows the 'Add permissions' configuration page. It lists a single policy:

Policy name	Type	Description
AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via th...

Below the table, there is a note: ▶ Set permissions boundary - optional

At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

- Define the role name, review it and finally create the role.

Cloud Computing

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
Admin
Maximum 64 characters. Use alphanumeric and '+,-,@,_' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+,-,@,_' characters.

Step 1: Select trusted entities

Trust policy

```
1 [ {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Action": [  
7                 "sts:AssumeRole"  
8             ],  
9             "Principal": {  
10                "Service": [  
11                    "ec2.amazonaws.com"  
12                ]  
13            }  
14        }  
15    ]  
16 }]
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonEC2FullAccess	AWS managed	Permissions policy

⌚ Role Admin created.

View role X

Roles (6) 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.

C Delete Create role

Search

Role name	Trusted entities	Last activity
ecsTaskExecutionRole	AWS Service: ecs-tasks	Yesterday

Cloud Computing

The screenshot shows the 'Summary' tab for a new IAM role named 'Admin'. It includes details like creation date (October 18, 2023), last activity (Yesterday), ARN (arn:aws:iam::547272956667:role/ecsTaskExecutionRole), and maximum session duration (1 hour). Below the summary, there are tabs for 'Permissions', 'Trust relationships', 'Tags', 'Access Advisor', and 'Revoke sessions'. The 'Permissions' tab is selected, showing one attached policy: 'AmazonECSTaskExecutionRolePolicy' (AWS managed). There are buttons for 'Edit', 'View role', and 'X' in the top right.

The screenshot shows the 'Admin' role's details page. It includes a summary table with creation date (October 26, 2023), last activity (empty), ARN (arn:aws:iam::547272956667:role/Admin), and instance profile ARN (arn:aws:iam::547272956667:instance-profile/Admin). Below the summary, there are tabs for 'Permissions', 'Trust relationships', 'Tags', 'Access Advisor', and 'Revoke sessions'. The 'Trust relationships' tab is selected, showing the JSON trust policy:

```
1 [{}]
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Service": "ec2.amazonaws.com"
8     },
9     {
10      "Action": "sts:AssumeRole"
11    }
12 ]
```

Problem 6:- Demonstration Elastic Load balancing using ECS in AWS Tasks

Sandeep Wadhawan (01411604422)

Step 1: Configure a target group

Step 2: Register targets

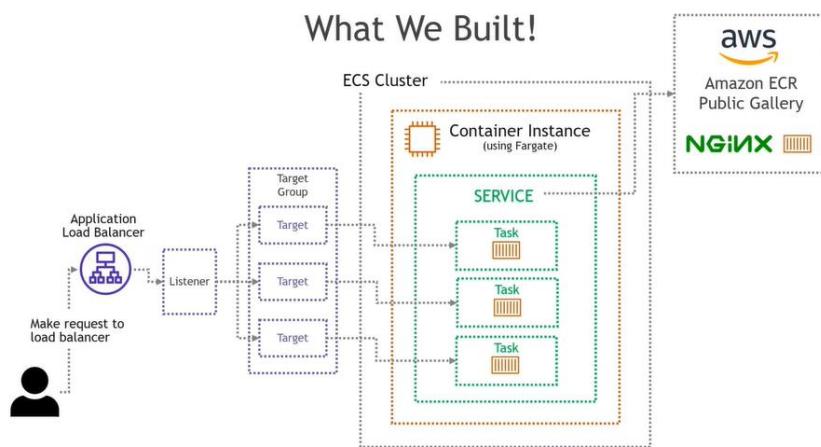
Step 3: Configure a load balancer and a listener

Step 4: Test the load balancer

Solution:-

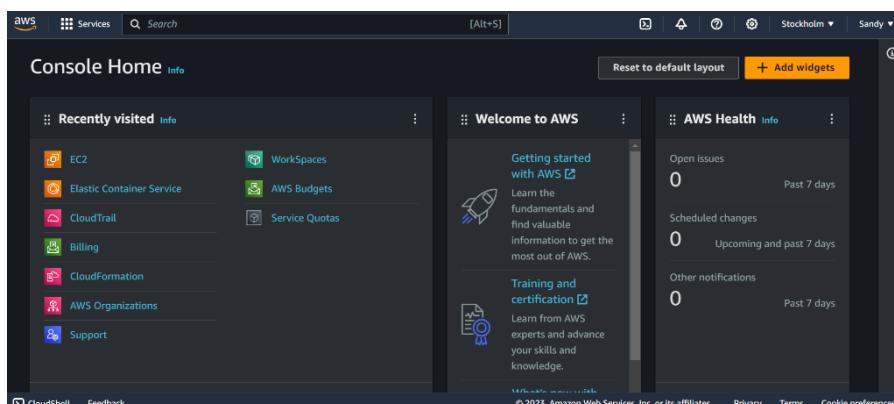
To demonstrate Elastic Load Balancing (ELB) using Amazon Elastic Container Service (ECS) in AWS, you'll set up a basic architecture where an application hosted on ECS containers is load balanced by an Application Load Balancer (ALB).

So, here is the working that we are building:



Here are the steps to achieve this:

1. Sign in to AWS: Log in to your AWS Management Console.



2. Create two Security Groups:

Cloud Computing

- One for the load balancer, accepting inbound traffic, Port 80 from anywhere.

The screenshot shows the AWS EC2 'Create security group' interface. In the 'Basic details' section, the security group name is 'ApplicationLoadBalancerSecurityGroup' and the description is 'Inbound traffic, Port 80 from anywhere'. A VPC is selected. In the 'Inbound rules' section, a new rule is being configured with Type: HTTP, Protocol: TCP, Port range: 80, and Source: Anywhere. A success message at the bottom indicates the group was created successfully. Below this, the 'sg-084f43230d28324dc - ApplicationLoadBalancerSecurityGroup' page is shown, displaying its details and the newly created inbound rule.

EC2 > Security Groups > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
ApplicationLoadBalancerSecurityGroup

Name cannot be edited after creation.

Description [Info](#)
Inbound traffic, Port 80 from anywhere

VPC [Info](#)
Q vpc-012951894c0a7787c

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
HTTP	TCP	80	Anywhere... ▾	<input type="text"/> 0.0.0.0/0 X

⌚ Security group (sg-084f43230d28324dc | ApplicationLoadBalancerSecurityGroup) was created successfully
► Details

EC2 > Security Groups > sg-084f43230d28324dc - ApplicationLoadBalancerSecurityGroup

sg-084f43230d28324dc - ApplicationLoadBalancerSecurityGroup

Details

Security group name ApplicationLoadBalancerSecurityGroup	Security group ID sg-084f43230d28324dc	Description Inbound traffic, Port 80 from anywhere	VPC ID vpc-012951894c0a7787c
Owner 547272956667	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules [Manage tags](#) [Edit inbound rules](#)

Inbound rules (1/1)											
<input type="text"/> Filter security group rules											
Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description	Actions	◀	▶	✖
-	sgr-0e24e30f7845b0b5d	IPv4	HTTP	TCP	80	0.0.0.0/0	-	Edit	<	1	>

- One for the service/containers, accepting inbound traffic from the load balancer.

The screenshot shows the AWS EC2 'Create security group' interface. In the 'Basic details' section, the security group name is 'ContainerFromALBSecurityGroup' and the description is 'Inbound traffic from ApplicationLoadBalancerSecurityGroup'. A VPC is selected. In the 'Inbound rules' section, a new rule is being configured with Type: All TCP, Protocol: TCP, Port range: 0 - 65535, and Source: sg-084f43230d28324dc. An 'Add rule' button is visible at the bottom.

EC2 > Security Groups > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
ContainerFromALBSecurityGroup

Name cannot be edited after creation.

Description [Info](#)
Inbound traffic from ApplicationLoadBalancerSecurityGroup

VPC [Info](#)
Q vpc-012951894c0a7787c

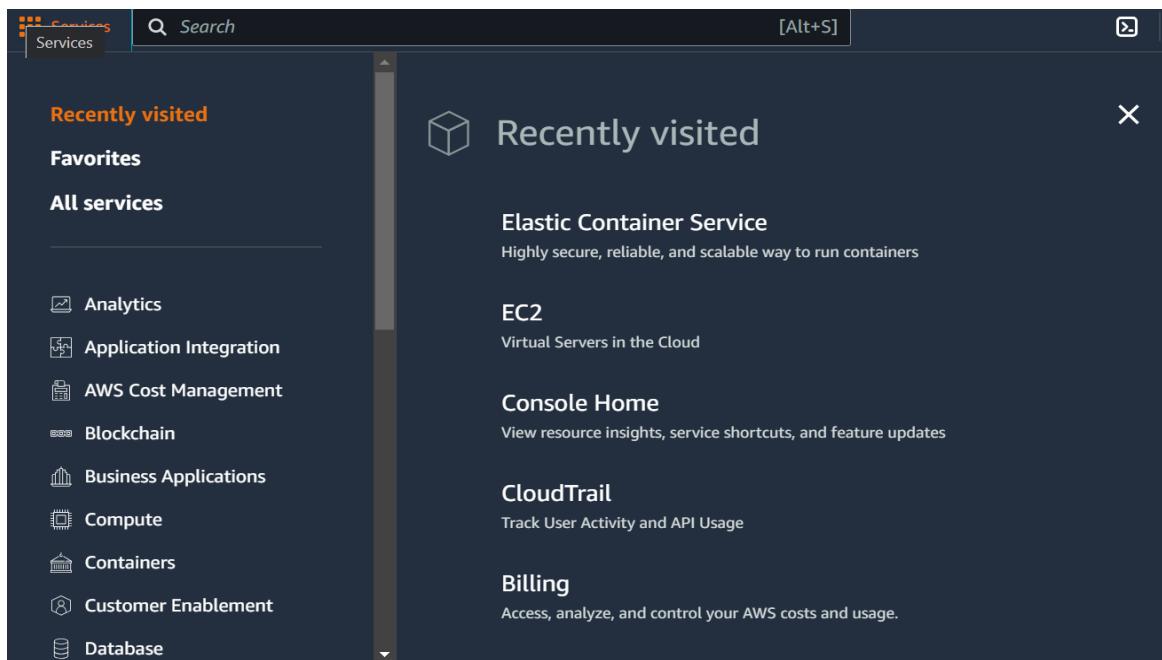
Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
All TCP	TCP	0 - 65535	Custom ▾	<input type="text"/> sg-084f43230d28324dc X

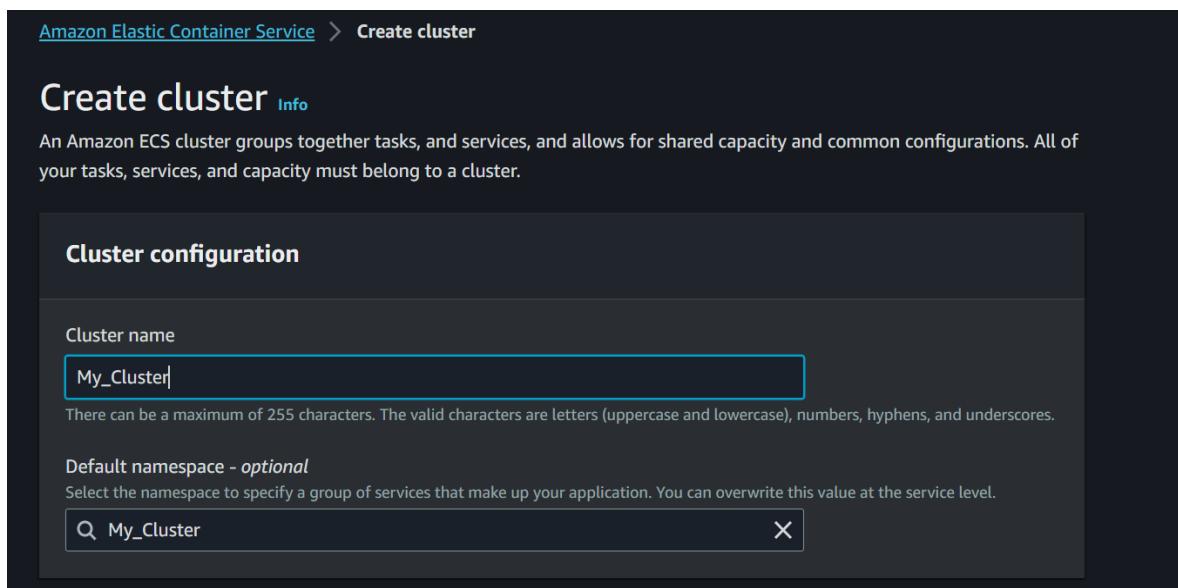
[Add rule](#)

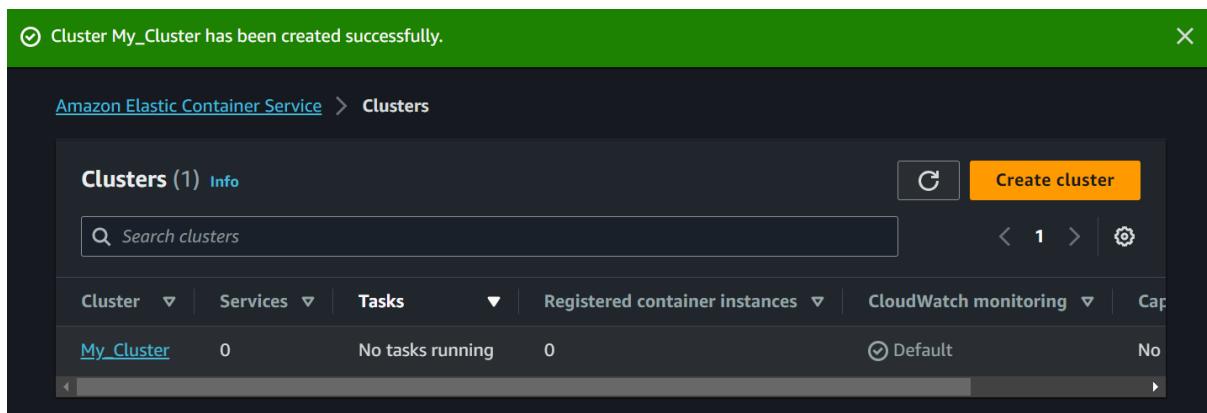
3. Create an ECS Cluster:

- Go to services and search “ECS (Elastic Container Service)”.



- Click on Create cluster.





4. Create a new task definition for nginx.

The screenshot shows the "Create new task definition" page. The first section, "Task definition configuration", includes a field for the "Task definition family" named "nginx-task-definition". The second section, "Infrastructure requirements", specifies the launch type as "AWS Fargate". The "Operating system/Architecture" section shows "Linux/X86_64" selected. The "Network mode" is set to "awsvpc". Under "Task size", the CPU is ".5 vCPU" and Memory is "3 GB". The final section, "Task roles - conditional", indicates that a task IAM role allows API requests to AWS services, with a note about creating it via the IAM console.

Cloud Computing

Container - 1 [Info](#)

Container details
Specify a name, container image, and whether the container should be marked as essential. Each task definition must have at least one essential container.

Name	Image URI	Essential container
nginx	public.ecr.aws/nginx/nginx:mainline	Yes

Private registry [Info](#)
Store credentials in Secrets Manager, and then use the credentials to reference images in private registries.

Private registry authentication

Port mappings [Info](#)
Add port mappings to allow the container to access ports on the host to send or receive traffic. Any changes to port mappings configuration impacts the associated service connect settings.

Container port	Protocol	Port name	App protocol
80	TCP	nginx-80-tcp	HTTP
Remove			

[Add port mapping](#)

Read only root file system [Info](#)
When this parameter is turned on, the container is given read-only access to its root file system.

Read only

Resource allocation limits - conditional [Info](#)
Container-level CPU, GPU, and memory limits are different from task-level values. They define how much resources are allocated for the container. If container attempts to exceed the memory specified in hard limit, the container is terminated.

CPU	GPU	Memory hard limit	Memory soft limit
-----	-----	-------------------	-------------------

⌚ Task definition successfully created
nginx-task-definition:3 has been successfully created. You can use this task definition to deploy a service or run a task.

[Deploy](#) [X](#)

[Amazon Elastic Container Service](#) > [Task definitions](#) > [nginx-task-definition](#) > [Revision 3](#) > [Containers](#)

nginx-task-definition:3

[Deploy](#) [Actions](#) [Create new revision](#)

Overview [Info](#)

ARN arn:aws:ecs:eu-north-1:54727295:task-definition/nginx-task-definition:3	Status ACTIVE	Time created 2023-10-25T07:24:11.529Z	App environment FARGATE
Task role -	Task execution role ecsTaskExecutionRole	Operating system/Architecture Linux/X86_64	Network mode awsvpc

5. Deploy the ECS service

My_Cluster

[C](#) [Update cluster](#) [Delete cluster](#)

Cluster overview

ARN arn:aws:ecs:eu-north-1:54727295:cluster/My_Cluster	Status Active	CloudWatch monitoring Default	Registered container instances -
---	----------------------------------	--	-------------------------------------

Services

Draining -	Active -	Pending -	Running -
---------------	-------------	--------------	--------------

Tasks

Pending -	Running -
--------------	--------------

[Services](#) [Tasks](#) [Infrastructure](#) [Metrics](#) [Scheduled tasks](#) [Tags](#)

Services (0) [Info](#)

[C](#) [Manage tags](#) [Update](#) [Delete service](#) [Create](#)

Filter launch type [Any launch type](#) Filter service type [Any service type](#)

[Filter services by value](#)

Sandeep Wadhawan (01411604422)

Cloud Computing

Deployment configuration

Application type | Info
Specify what type of application you want to run.

Service
Launch a group of tasks handling a long-running computing work that can be stopped and restarted. For example, a web application.

Task
Launch a standalone task that runs and terminates. For example, a batch job.

Task definition
Select an existing task definition. To create a new task definition, go to [Task definitions](#).
 Specify the revision manually
Manually input the revision instead of choosing from the 100 most recent revisions for the selected task definition family.

Family nginx-task-definition Revision 3 (LATEST)

Service name
Assign a unique name for this service.
NginxWithALBService

Service type | Info
Specify the service type that the service scheduler will follow.

Replica
Place and maintain a desired number of tasks across your cluster.

Daemon
Place and maintain one copy of your task on each container instance.

Desired tasks
Specify the number of tasks to launch.
3

Networking

VPC | Info
Choose the Virtual Private Cloud to use.
vpc-012951894c0a7787c default

Subnets
Choose the subnets within the VPC that the task scheduler should consider for placement.
Choose subnets

subnet-0639908be9e5aa73c X eu-north-1c 172.31.0.0/20
subnet-0203fc76ed9897b18 X eu-north-1a 172.31.16.0/20
subnet-092f1de7f780339da X eu-north-1b 172.31.32.0/20

Security group | Info
Choose an existing security group or create a new security group.
 Use an existing security group
 Create a new security group
Security group name
Choose an existing security group.
Choose security groups

sg-047ffeb4accdddb6 X ContainerFromALBSecurityGroup

Public IP | Info
Choose whether to auto-assign a public IP to the task's elastic network interface (ENI).
 Turned on

6. Create the Load Balancer to work with ECS service

▼ Load balancing - optional

Load balancer

Load balancer type | [Info](#)
Configure a load balancer to distribute incoming traffic across the tasks running in your service.

Application Load Balancer

Application Load Balancer
Specify whether to create a new load balancer or choose an existing one.

- Create a new load balancer
- Use an existing load balancer

Load balancer name
Assign a unique name for the load balancer.

Load-Balancer-for-nginx-ECS

Health check grace period | [Info](#)

20
seconds

Container

Choose container to load balance

nginx 80:80

Listener | [Info](#)
Specify the port and protocol that the load balancer will listen for connection requests on.

- Create new listener
- Use an existing listener
You need to select an existing load balancer.

Port
80

Protocol
HTTP

Target group | [Info](#)
Specify whether to create a new target group or choose an existing one that the load balancer will use to route requests to the tasks in your service.

- Create new target group
- Use an existing target group
You need to select an existing load balancer.

Target group name
nginx-target-group

Protocol
HTTP

Health check protocol
HTTP

Health check path | [Info](#)

/

Services (1) Info		C	Manage tags	Update	Delete service	Create
		Filter launch type	Filter service type			
<input type="text"/> Filter services by value		<input type="button"/> Any launch type	<input type="button"/> Any service type	< 1 > @		
<input type="checkbox"/>	Service name	<input type="button"/> Status	<input type="button"/> ARN	<input type="button"/> Service type	<input type="button"/> Deployments and tasks	<input type="button"/> Last deploy... Task defin... Revision
<input type="checkbox"/>	NginxWithALBService	<input checked="" type="radio"/> Active	<input type="button"/> arn:aws:se...	REPLICA	<div style="width: 100%;"><div style="width: 100%;">3/3 Tasks ru...</div></div>	<input type="button"/> In progress nginx-task-de... 3

7. Testing our Load Balancer

- Go to EC2 dashboard and click on “Load Balancers”.

The screenshot shows the AWS EC2 Load Balancers page. At the top, there is a breadcrumb navigation: EC2 > Load balancers. Below the header, a message states: "Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic." A search bar labeled "Filter load balancers" is present. To the right of the search bar are buttons for "Actions" and "Create load balancer". The main area displays a table with the following columns: Name, DNS name, State, VPC ID, Availability Zones, Type, and Date created. One row is visible in the table:

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
Load-Balancer-for-nginx-ECS	Load-Balancer-for-nginx-ECS	Active	vpc-012951894c0a7787c	3 Availability Zones	application	October 25, 2022

- Edit the security type i.e. change the security group from Container ALB Group to Application Load Balancer Security group.

The screenshot shows the "Edit security groups" dialog for the "Load-Balancer-for-nginx-ECS" load balancer. At the top, there is a breadcrumb navigation: EC2 > Load balancers > Load-Balancer-for-nginx-ECS > Edit security groups. The title of the dialog is "Edit security groups". Below the title, a section titled "Load balancer details: Load-Balancer-for-nginx-ECS" is shown. The next section is "Security groups", which contains the following text: "A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group [?].". A dropdown menu titled "Select up to 5 security groups" is open, showing a single item: "ApplicationLoadBalancerSecurityGroup sg-084f43230d28324dc VPC: vpc-012951894c0a7787c". At the bottom of the dialog are two buttons: "Cancel" and "Save changes".

- Copy the DNS name

Cloud Computing

Load balancer type: Application
Status: Active
VPC: vpc-012951894c0a7787c
IP address type: IPv4
Scheme: Internet-facing
Hosted zone: Z23TAZ6LKFMNIO
Availability Zones: eu-north-1c (eun1-az3), eu-north-1a (eun1-az1), eu-north-1b (eun1-az2)
Date created: October 25, 2023, 13:43 (UTC+05:30)
Load balancer ARN: arn:aws:elasticloadbalancing:eu-north-1:547272956667:loadbalancer/app/Load-Balancer-for-nginx-ECS/c268fb66c2f6a84f
DNS name copied: Load-Balancer-for-nginx-ECS-1435371612.eu-north-1.elb.amazonaws.com (A Record)

- Paste it in incognito mode and we'll see a web page of nginx.

