

AWS EC2 INSTANCE TASK

Name: Aakash Namala

Roll No: 20A91A0544

Create an ec2 instance with the ubuntu operating system, set all the required parameters such as security groups and key pair, and also do SSH with git bash to the running instance.

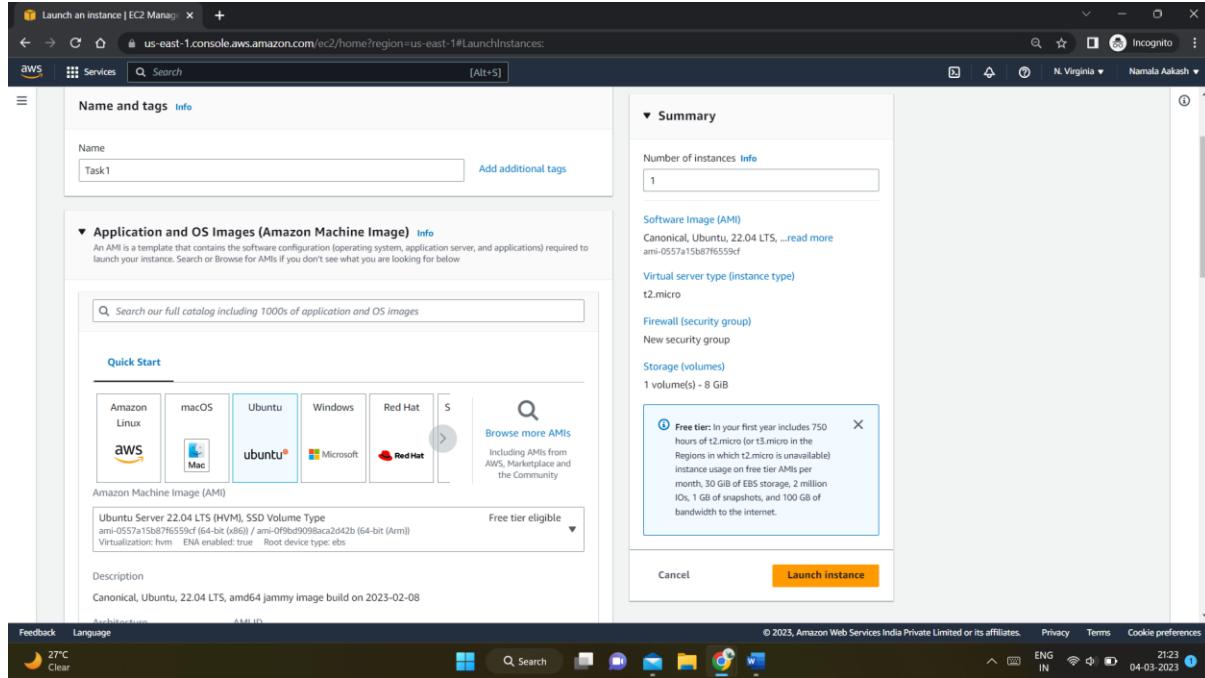
Also, install NodeJS on top of the instance and check for the version of node to cross-check if NodeJS is installed successfully.

Also, configure the instance with an elastic ip to show the static public ip address.

Also, create an S3 bucket and upload an object to it and show the object URL for reference.

Step 1:

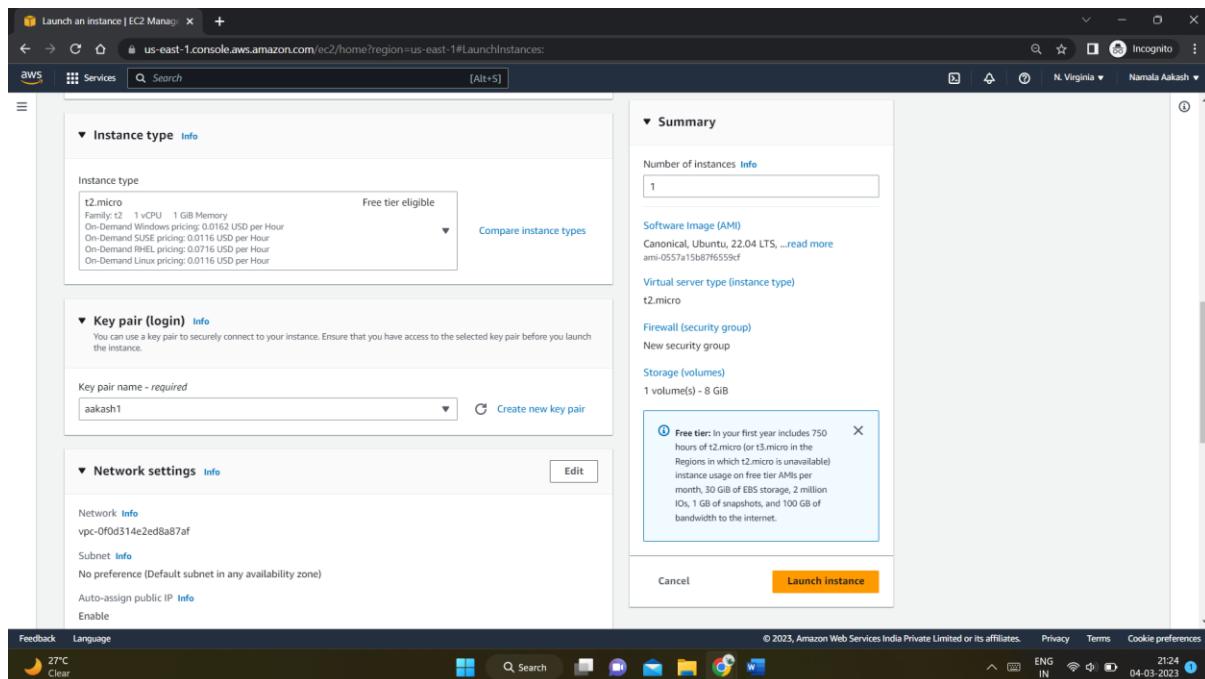
Go to launch the Instance. Add name of the instance and select the AMI for your instance. Here we are selecting Ubuntu AMI.



The screenshot shows the AWS EC2 Launch Instance wizard. In the 'Name and tags' step, the instance is named 'Task1'. The 'Application and OS Images (Amazon Machine Image)' section shows a search bar and a 'Quick Start' grid with categories like Amazon Linux, macOS, Ubuntu, Windows, and Red Hat. A detailed view of the 'Ubuntu Server 22.04 LTS (HVM), SSD Volume Type' AMI is shown, including its AMI ID (ami-0557a15b87f6559cf), Virtualization type (hvm), ENA enabled status, and Root device type (ebs). The 'Summary' panel indicates 1 instance will be launched with the Canonical, Ubuntu, 22.04 LTS AMI. A tooltip for the free tier is visible, stating it includes 750 hours of t2.micro or t3.micro usage per month. The bottom right contains a 'Launch instance' button.

Step 2:

Select the instance type and key pair for your instance. If you don't have a key, create a new key pair.



The screenshot shows the AWS EC2 Launch Instance wizard. In the 'Instance type' step, 't2.micro' is selected. In the 'Key pair (login)' step, 'aakash' is chosen as the key pair name. In the 'Network settings' step, the network and subnet are specified. The 'Summary' panel indicates 1 instance will be launched with the selected t2.micro instance type. A tooltip for the free tier is visible, stating it includes 750 hours of t2.micro usage per month. The bottom right contains a 'Launch instance' button.

Step 3:

Configure the network settings.

This includes the security groups and VPC settings.

VPC - required Info
VPC-0f0d314e2ed8a87af (default)
Subnet Info
No preference Create new subnet
Auto-assign public IP Info
Enable

Firewall (security group) 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

Security group name - required
launch-wizard-3

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, _-/[!@#%^&{}|=]{}

Description - required Info
launch-wizard-3 created 2023-03-04T15:53:29.679Z

Inbound security groups rules

Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type Info	Protocol Info	Port range Info
ssh	TCP	22

Source type Info
Anywhere

Description - optional Info
e.g. SSH for admin desktop

Remove

Cancel Launch instance

Step 4:

Now launch the instance.

Success
Successfully initiated launch of instance (i-0dbc8b60d1fea2e80)

▶ Launch log

Next Steps - preview

What would you like to do next with this instance, for example "create alarm" or "create backup"

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
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

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots.
Create EBS snapshot policy

Feedback Language
27°C Clear © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 21:24 04-03-2023

Now view the instance in the instance dashboard.

The screenshot shows the AWS EC2 Management Console. The left sidebar is collapsed. The main area displays the 'Instances (1/1) info' table with one row for 'Task1'. The table columns include Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. Below the table, the 'Instance: i-0dbc8b60d1fea2e80 (Task1)' details page is open. The 'Details' tab is selected, showing the following information:

Attribute	Value
Instance ID	i-0dbc8b60d1fea2e80 (Task1)
IPv6 address	-
Hostname type	IP name: ip-172-31-87-244.ec2.internal
Answer private resource DNS name	IPV4 (A)
Auto-assigned IP address	-
Public IPv4 address	3.88.115.195 open address
Instance state	Running
Private IP DNS name (IPv4 only)	ip-172-31-87-244.ec2.internal
Instance type	t2.micro
VPC ID	-

Now select the instance and tap on connect. Now go to the ssh client, copy the command

The screenshot shows the 'Connect to instance' dialog for the instance i-0dbc8b60d1fea2e80. The 'SSH client' tab is selected. The dialog contains the following text:

Connect to your instance i-0dbc8b60d1fea2e80 (Task1) using any of these options

EC2 Instance Connect | Session Manager | **SSH client** | EC2 serial console

Instance ID: i-0dbc8b60d1fea2e80 (Task1)

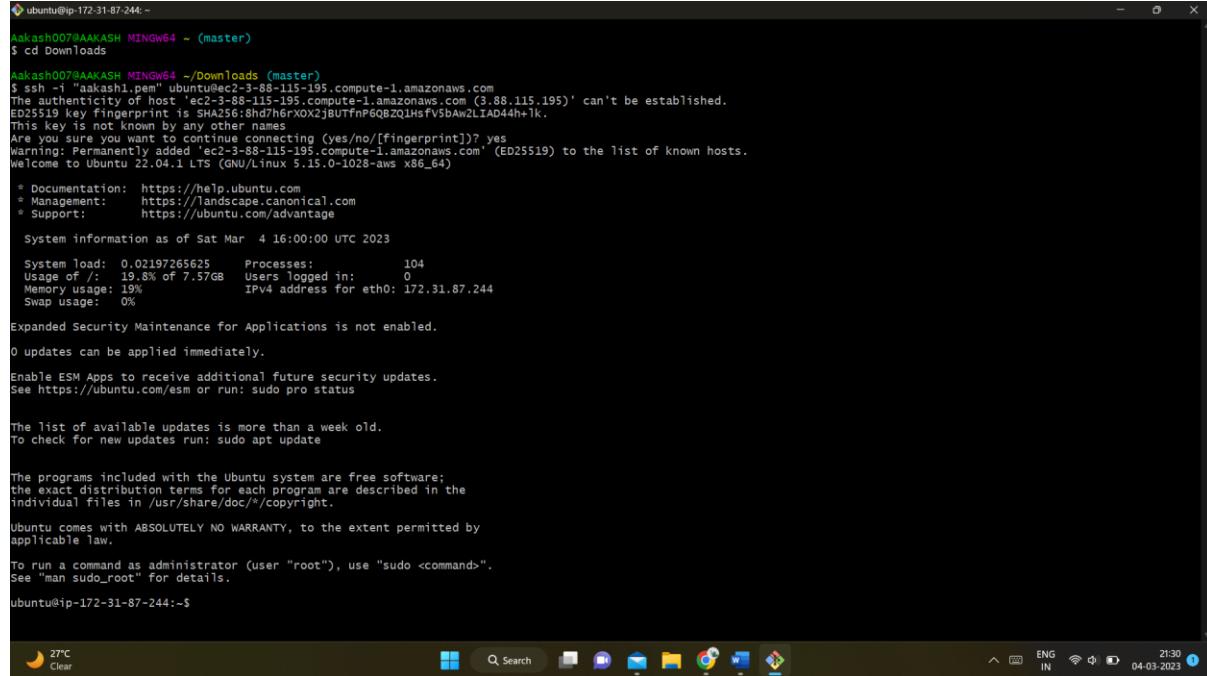
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is aakash1.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 chmod 400 aakash1.pem
4. Connect to your instance using its Public DNS:
 ec2-3-88-115-195.compute-1.amazonaws.com

Example:
ssh -i "akash1.pem" ubuntu@ec2-3-88-115-195.compute-1.amazonaws.com

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

Now Open Git Bash and move to the directory that is having the pem. And past the command.

```
ssh -i "akash1.pem" ubuntu@ec2-3-88-115-195.compute-1.amazonaws.com
```



```
Aakash007@AKASH MINGW64 ~ (master)
$ cd Downloads
Aakash007@AKASH MINGW64 ~ (master)
$ ssh -i "akash1.pem" ubuntu@ec2-3-88-115-195.compute-1.amazonaws.com
The authenticity of host 'ec2-3-88-115-195.compute-1.amazonaws.com (3.88.115.195)' can't be established.
ED25519 key fingerprint is SHA256:8hd7h6rXOX2jBUTfnP6QBZQ1Hsfv5bAw2LIAAD4h+1k.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-88-115-195.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1028-aws x86_64)

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

 System information as of Sat Mar 4 16:00:00 UTC 2023

 System load: 0.02197265625 Processes: 104
 Usage of /: 19.8% of 7.57GB Users logged in: 0
 Memory usage: 19% IPv4 address for eth0: 17.31.87.244
 Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

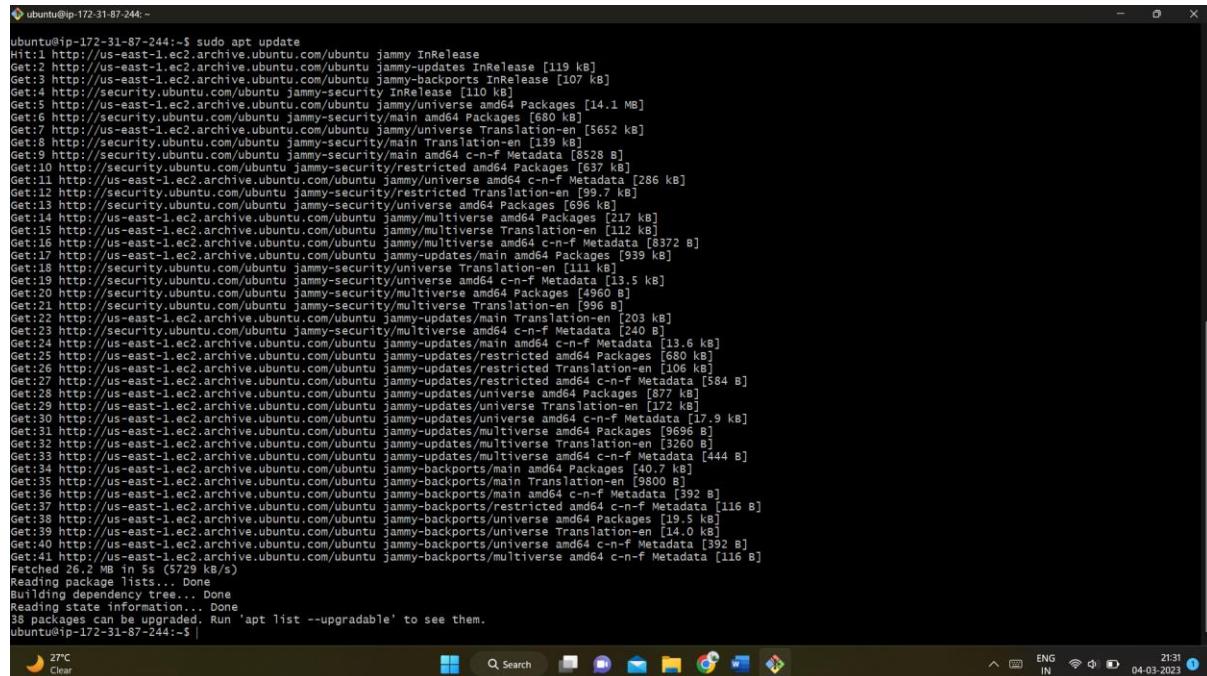
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-87-244:~
```

Now use the commands to install nodejs.

“sudo apt update”

“sudo apt install nodejs”



```
ubuntu@ip-172-31-87-244:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 kB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [65 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [5652 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [139 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [8528 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy/universe restricted amd64 Packages [637 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [99.7 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [699 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates amd64 c-n-f Metadata [8372 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [639 kB]
Get:18 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [111 kB]
Get:19 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [13.5 kB]
Get:20 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [4960 kB]
Get:21 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [996 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [203 kB]
Get:23 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [249 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [13.6 kB]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [160 kB]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [106 kB]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [584 kB]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [677 kB]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [172 kB]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [17.9 kB]
Get:31 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [9696 kB]
Get:32 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [3260 kB]
Get:33 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [444 kB]
Get:34 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [40.7 kB]
Get:35 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [6881 kB]
Get:36 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [392 kB]
Get:37 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 kB]
Get:38 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [19.5 kB]
Get:39 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [14.0 kB]
Get:40 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [392 kB]
Get:41 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 kB]
Fetched 26.2 MB in 5s (5729 kB/s)
Reading package lists... Done
Building dependency tree... Done
Resolving dependencies... Done
38 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-87-244:~
```

```

ubuntu@ip-172-31-87-244:~$ Building dependency tree... Done
Reading state information... Done
38 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-87-244:~$ sudo apt install nodejs
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  javascript-common libc-ares2 libjs-highlight.js libnode72 nodejs-doc
Suggested packages:
  apache2 | lighttpd | httpd npm
The following NEW packages will be installed:
  javascript-common libc-ares2 libjs-highlight.js libnode72 nodejs-doc
0 upgraded, 38 newly installed, 0 to remove and 38 not upgraded.
Need to get 13.7 MB of archives.
After this operation, 53.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 javascript-common all 11+nmui [5936 B]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 libjs-highlight.js all 9.18.5+dfsg1-1 [367 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 libc-ares2 amd64 1.18.1-1ubuntu0.22.04.1 [45.1 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 libnode72 amd64 12.22.9+dfsg-ubuntu3 [10.8 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 nodejs-doc all 12.22.9+dfsg-ubuntu3 [2409 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 nodejs amd64 12.22.9+dfsg-ubuntu3 [122 kB]
Fetched 13.7 MB in 0s (42.3 MB/s)
Selecting previously unselected package javascript-common.
(Reading database ... 63605 files and directories currently installed.)
Preparing to unpack .../0-javascript-common_11+nmui_all.deb ...
Unpacking javascript-common (11+nmui) ...
Selecting previously unselected package libjs-highlight.js.
Preparing to unpack .../1-libjs-highlight.js_9.18.5+dfsg1-1_all.deb ...
Unpacking libjs-highlight.js (9.18.5+dfsg1-1) ...
Selecting previously unselected package libc-ares2:amd64.
Preparing to unpack .../2-libc-ares2_1.18.1-1ubuntu0.22.04.1_amd64.deb ...
Unpacking libc-ares2:amd64 (1.18.1-1ubuntu0.22.04.1) ...
Selecting previously unselected package libnode72:amd64.
Preparing to unpack .../3-libnode72_12.22.9+dfsg-ubuntu3_amd64.deb ...
Unpacking libnode72:amd64 (12.22.9+dfsg-ubuntu3) ...
Selecting previously unselected package nodejs-doc.
Preparing to unpack .../4-nodejs-doc_12.22.9+dfsg-ubuntu3_all.deb ...
Unpacking nodejs-doc (12.22.9+dfsg-ubuntu3) ...
Selecting previously unselected package nodejs.
Preparing to unpack .../5-nodejs_12.22.9+dfsg-ubuntu3_amd64.deb ...
Unpacking nodejs (12.22.9+dfsg-ubuntu3) ...
Setting up javascript-common (11+nmui) ...
Setting up libc-ares2:amd64 (1.18.1-1ubuntu0.22.04.1) ...
Setting up libnode72:amd64 (12.22.9+dfsg-ubuntu3) ...
Setting up nodejs (12.22.9+dfsg-ubuntu3) ...
Setting up alternatives: using /usr/bin/nodejs to provide /usr/bin/js (js) in auto mode

```

Now to check the version of the nodejs, use the command “node -v”.

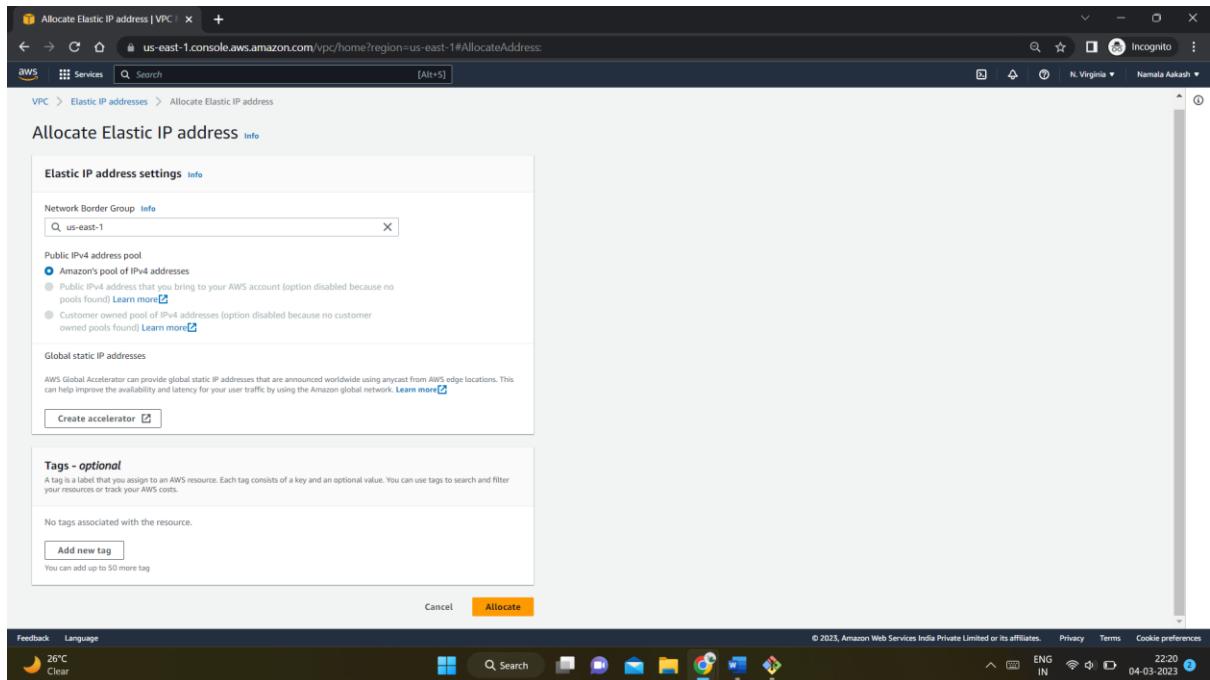
```

ubuntu@ip-172-31-87-244:~$ node -v
v12.22.9
ubuntu@ip-172-31-87-244:~$

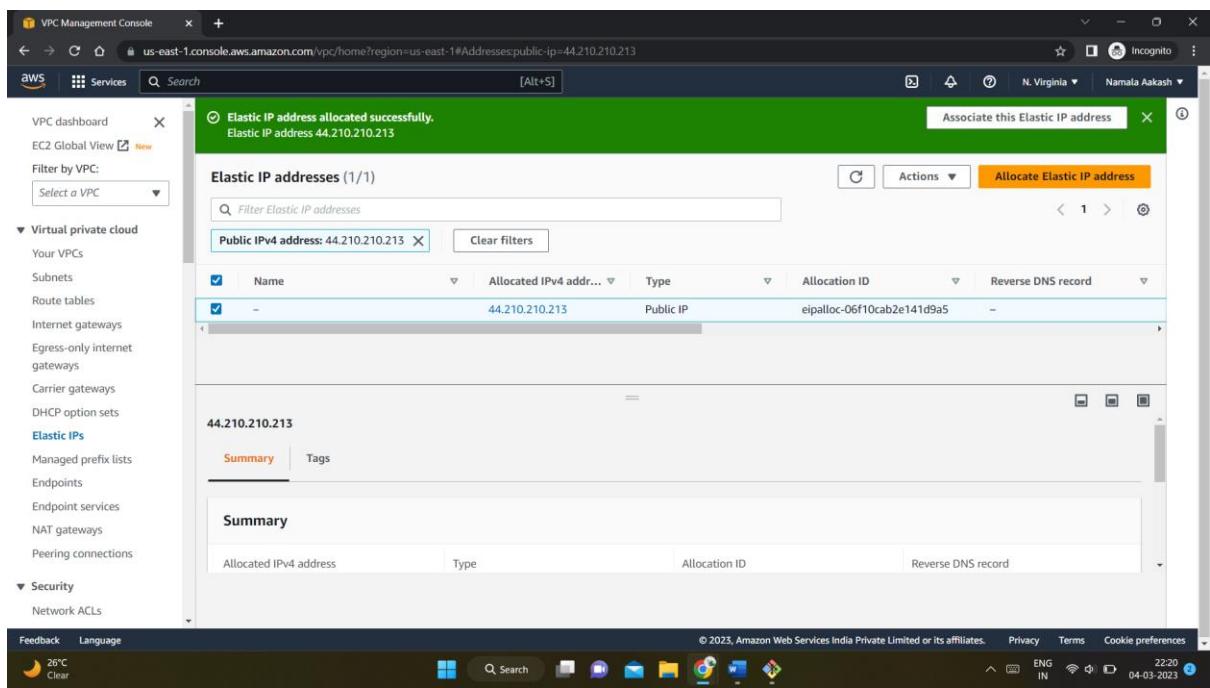
```

Now, to allocate IP address, go to elastic IP address

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record
				No Elastic IP addresses found



After creating the Elastic IP, view it in the dashboard.



Connect the instance to the elastic IP.

The screenshot shows the AWS VPC console interface. The user is navigating through the VPC service to associate an Elastic IP address (44.210.210.213) with an instance (i-0dbc8b60d1fea2e80). The private IP address specified is 172.31.87.244. A warning message states: "If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. Learn more." The "Associate" button is highlighted in orange at the bottom right of the form.

Elastic IP address: 44.210.210.213

Resource type:
Choose the type of resource with which to associate the Elastic IP address.
 Instance
 Network interface

Reassociation:
Specify whether the Elastic IP address can be reassigned with a different resource if it already associated with a resource.
 Allow this Elastic IP address to be reassigned

Cancel **Associate**

Elastic IP address associated successfully.
Elastic IP address 44.210.210.213 has been associated with instance i-0dbc8b60d1fea2e80

Summary

Allocated IPv4 address	Type	Allocation ID	Reverse DNS record
44.210.210.213	Public IP	eipalloc-06f10cab2e141d9a5	-
Association ID	Scope	Associated instance ID	Private IP address
eipassoc-0fd9a36bf8ea895c	VPC	i-0dbc8b60d1fea2e80	172.31.87.244
Network interface ID	Network interface owner account ID	Public DNS	NAT Gateway ID
eni-09be45b93aae00c7b	623894141141	ec2-44-210-210-213.compute-1.amazonaws.com	-
Address pool	Network Border Group	Region	
Amazon	us-east-1	us-east-1	

Tags (0)

No tags associated with this resource
Click the Manage tags button to add your first tag

Manage tags

Feedback Language
26°C Clear

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences
ENG IN 22:23 04-03-2023

The screenshot shows the AWS EC2 Management Console. The main view displays a table of instances with one entry: 'Task1' (Instance ID: i-0dbc8b60d1fea2e80). The instance is listed as 'Running'. The details pane below shows the instance summary, including its Public IPv4 address (44.210.210.213), Private IPv4 address (172.31.87.244), and its instance type (t2.micro). The status check section indicates 2/2 checks passed with no alarms. The subnet ID is us-east-1a, and the Public IPv4 DNS is ec2-44-210-210-213.compute-1.amazonaws.com.

After creating and associating the Elastic IP,
Check the elastic Ip by connecting to the instance.

The screenshot shows the 'Connect to instance' dialog for the instance 'Task1'. It provides three connection methods: EC2 Instance Connect, Session Manager, and SSH client. The SSH client tab is selected. A message indicates that the instance ID 'i-0dbc8b60d1fea2e80 (Task1)' can be used to connect. Below this, a list of steps for connecting via SSH is provided, followed by a note about the AMI owner's user name. A copy button has been used to copy the SSH command: 'ssh -i "akash1.pem" ubuntu@ec2-44-210-210-213.compute-1.amazonaws.com'. A note at the bottom of the dialog states: 'Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.'

```

ubuntu@ip-172-31-87-244:~ 
Aakash007AAKASH MINGW64 ~/Downloads (master)
$ ssh -i "aakash1.pem" ubuntu@ec2-44-210-210-213.compute-1.amazonaws.com
The authenticity of host 'ec2-44-210-210-213.compute-1.amazonaws.com (44.210.210.213)' can't be established.
ED25519 key fingerprint is SHA256:8hd7h6rXo2jbUTfpG6BZQ1Hsfv5baw2LIAD44h+lk.
This host key is known by the following other names/addresses:
  -./ssh/known_hosts:4: ec2-3-88-115-195.compute-1.amazonaws.com
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-44-210-210-213.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1028-aws x86_64)

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

 System information as of Sat Mar 4 16:56:52 UTC 2023

 System load: 0.0          Processes:           106
 Usage of /: 23.1% of 7.57GB   Users logged in: 1
 Memory usage: 24%          IPV4 address for eth0: 172.31.87.244
 Swap usage: 0%

 * Introducing Expanded Security Maintenance for Applications.
 Receive updates to over 25,000 software packages with your
 Ubuntu Pro subscription. Free for personal use.

 https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

37 updates can be applied immediately,
18 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat Mar 4 16:06:22 2023 from 117.205.68.99
ubuntu@ip-172-31-87-244:~$ |
```

22:27 04-03-2023

S3 BUCKET

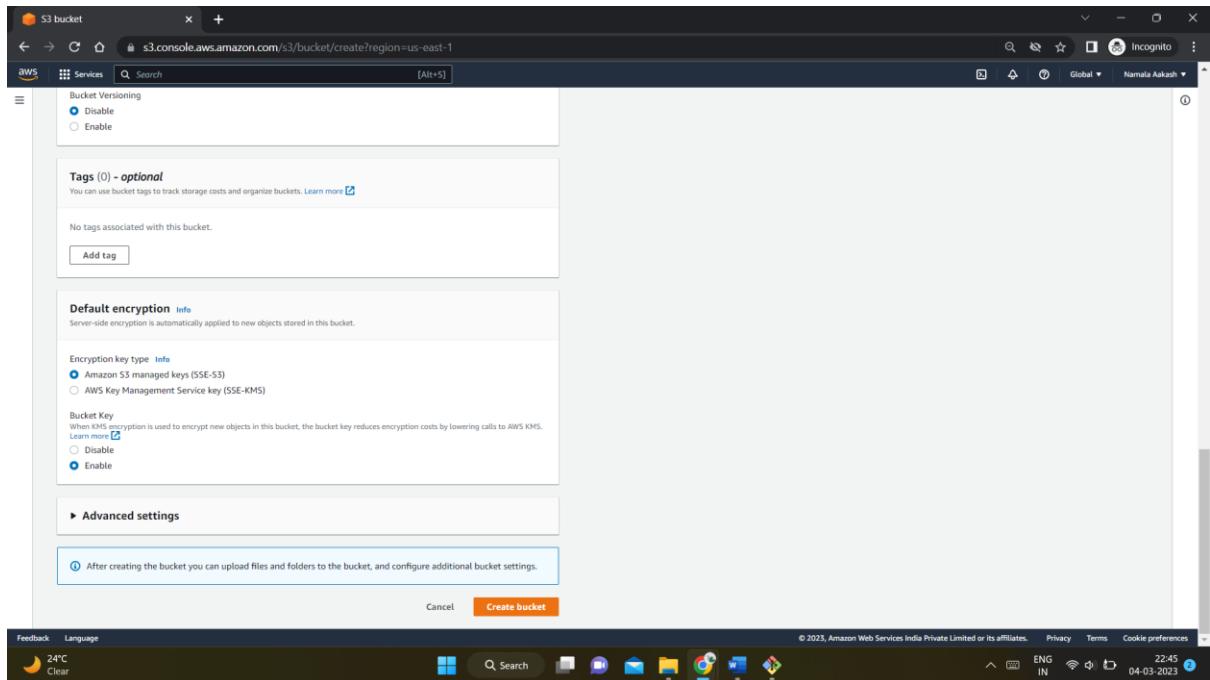
To create the s3 bucket, go s3 bucket and click on create bucket.

The screenshot shows the AWS S3 Management Console. The main page features the Amazon S3 logo and the tagline 'Store and retrieve any amount of data from anywhere'. A prominent 'Create a bucket' button is visible on the right. To the left, there's a 'How it works' section with a video thumbnail titled 'Introduction to Amazon S3'. On the right, there are sections for 'Pricing' (which states 'With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.') and 'Resources' (which includes links to 'User guide', 'API reference', 'FAQs', and 'Discussion forums'). The browser's address bar shows the URL 's3.console.aws.amazon.com/s3/get-started?region=us-east-1'. The desktop taskbar at the bottom shows various application icons and the system clock.

Now configure the bucket properties and settings.

The screenshot shows the 'Create bucket' page in the AWS S3 console. In the 'General configuration' section, the 'Bucket name' field is set to 'akash-task'. The 'AWS Region' dropdown is set to 'US East (N. Virginia) us-east-1'. Below this, there's a note about copying settings from an existing bucket, followed by a 'Choose bucket' button. The 'Object Ownership' section contains two options: 'ACLs disabled (recommended)' (selected) and 'ACLs enabled'. A note states that objects in the bucket are owned by the account. The 'Object Ownership' dropdown is set to 'Bucket owner enforced'. A warning message at the bottom indicates that starting in April 2023, the ability to disable ACLs will be removed. The browser status bar at the bottom shows the date as 04-03-2023.

The screenshot shows the 'Block Public Access settings for this bucket' page. It lists five settings: 'Block all public access', 'Block public access to buckets and objects granted through new access control lists (ACLS)', 'Block public access to buckets and objects granted through any access control lists (ACLS)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. The first setting, 'Block all public access', is selected. A warning message at the bottom states that turning off this setting might result in the bucket becoming public. A checkbox for acknowledging this risk is checked. A note at the bottom indicates that starting in April 2023, the ability to disable any Block Public Access setting will be removed. The browser status bar at the bottom shows the date as 04-03-2023.



The screenshot shows the 'Buckets' page in the AWS S3 Management Console. A green banner at the top says 'Successfully created bucket "akash-task"'. Below it, the 'Account snapshot' section provides visibility into storage usage and activity trends. The main table lists the single bucket 'akash-task' with details: Name (akash-task), AWS Region (US East (N. Virginia) us-east-1), Access (Objects can be public), and Creation date (March 4, 2023, 22:45:41 (UTC+05:30)).

Now upload the objects into the bucket.

The screenshot shows the AWS S3 console interface. On the left, a sidebar menu includes 'Buckets', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', and 'IAM Access Analyzer for S3'. Below these are sections for 'Block Public Access settings for this account', 'Storage Lens', 'Dashboards', 'AWS Organizations settings', 'Feature spotlight', and 'AWS Marketplace for S3'. The main content area displays the 'akash-task' bucket. It has tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Under the 'Objects' tab, there is a table with one row: 'No objects'. A message below the table says 'You don't have any objects in this bucket.' At the bottom right of the table is a large orange 'Upload' button. The browser's address bar shows the URL `s3.console.aws.amazon.com/s3/buckets/akash-task?region=us-east-1&tab=objects`. The status bar at the bottom right indicates the date as 04-03-2023 and the time as 22:48.

Upload the files. Drag the files you want to upload.

The screenshot shows the 'Upload' interface for the 'akash-task' bucket. The top navigation bar includes tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Below the tabs is a search bar and a 'Find objects by prefix' input field. A large orange 'Upload' button is prominently displayed. The main area shows a table titled 'Files and folders (80 Total, 7.8 MB)' with columns for 'Name', 'Folder', 'Type', and 'Size'. The table lists several files and folders, including '.DS_Store', 'about.html', 'animate.min.css', 'banner-bg.png', and 'blog.html'. Each item in the table has a checkbox next to it. At the bottom of the table is a 'Remove' button. The browser's address bar shows the URL `s3.console.aws.amazon.com/s3/upload/akash-task?region=us-east-1`. The status bar at the bottom right indicates the date as 04-03-2023 and the time as 23:10.

Screenshot of the AWS S3 Management Console showing the upload process for a website template.

Upload Progress:

File	Type	Size	Status
banner-bg.png	image/png	492.9 KB	Succeeded
blog.html	text/html	7.7 KB	Succeeded
bootstrap-grid.css	text/css	36.8 KB	Succeeded
bootstrap-grid.css.map	-	95.3 KB	Succeeded
bootstrap-grid.min.css	text/css	28.3 KB	Succeeded
bootstrap-grid.min.css.map	-	66.6 KB	Succeeded

Destination: s3://akash-task

Destination details: Bucket settings that impact new objects stored in the specified destination.

Permissions: Grant public access and access to other AWS accounts.

Properties: Specify storage class, encryption settings, tags, and more.

Upload Buttons: Cancel, Upload

Success Message: Upload succeeded. View details below.

Summary:

Destination	Succeeded	Failed
s3://akash-task	80 files, 7.8 MB (100.00%)	0 files, 0 B (0%)

Files and folders: (80 Total, 7.8 MB)

Name	Type	Size	Status	Error
.DS_Store	-	8.0 KB	Succeeded	-
.DS_Store	-	8.0 KB	Succeeded	-
about.html	text/html	6.4 KB	Succeeded	-
animate.min.css	text/css	52.4 KB	Succeeded	-
banner-bg.png	image/png	492.9 KB	Succeeded	-
blog.html	text/html	7.7 KB	Succeeded	-
bootstrap-grid.css	text/css	36.8 KB	Succeeded	-
bootstrap-grid.min.css	-	66.6 KB	Succeeded	-

Objects are added to the bucket.

Screenshot of the AWS S3 Bucket Permissions Overview page for 'akash-task' bucket.

Permissions overview

Access
Objects can be public

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](#)

Edit

Block all public access

Off

Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

No policy to display.

[Edit](#) [Delete](#) [Copy](#)

<https://s3.console.aws.amazon.com/s3/#>

24°C Clear

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 23:13 04-03-2023

Screenshot of the AWS S3 Bucket Policy editor for 'akash-task' bucket.

Bucket ARN

arn:aws:s3:::akash-task

Policy

```

1 - {
2   "version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": "s3:GetObject",
9       "Resource": [
10         "arn:aws:s3:::akash-task/*"
11       ]
12     }
13   ]
14 }
15 }
```

Edit statement **Remove**

1. Add actions

Choose a service

Included 53

Available

- AMP
- API Gateway
- API Gateway V2
- ASC
- Access Analyzer
- Account
- Activate
- Alexa for Business
- Amplify

2. Add a resource **Add**

3. Add a condition (optional) **Add**

[+ Add new statement](#)

JSON Ln 13, Col 13

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

[Preview external access](#)

[Cancel](#) [Save changes](#)

<https://s3.console.aws.amazon.com/s3/#>

24°C Clear

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 23:14 04-03-2023

Screenshot of the AWS S3 console showing the contents of the 'html/' folder. The 'index.html' file is selected.

Name	Type	Last modified	Size	Storage class
about.html	html	March 4, 2023, 23:10:57 (UTC+05:30)	6.4 KB	Standard
blog.html	html	March 4, 2023, 23:10:58 (UTC+05:30)	7.7 KB	Standard
client.html	html	March 4, 2023, 23:10:59 (UTC+05:30)	12.7 KB	Standard
contact.html	html	March 4, 2023, 23:11:00 (UTC+05:30)	7.1 KB	Standard
css/	Folder	-	-	-
images/	Folder	-	-	-
index.html	html	March 4, 2023, 23:11:01 (UTC+05:30)	26.3 KB	Standard
js/	Folder	-	-	-
services.html	html	March 4, 2023, 23:11:02 (UTC+05:30)	9.3 KB	Standard

Screenshot of a web browser displaying a professional consulting website. The main heading is 'WE ARE PROVIDE PROFESSIONAL CONSULTING'.

It is a long established fact that a reader will be distracted by the readable content of a page

[Read More](#) [Get A Quote](#)

[SEE CONSULTING VIDEOS](#)

