

Documentation 1

Deploy a basic HTML/CSS Website on AWS EC2 Using Apache

Step 1: Launch an Ubuntu EC2 Instance

1. **Log in to the AWS Console** and navigate to the EC2 Dashboard.
2. **Launch an Instance:**
 - **AMI:** Select **Ubuntu Server 24.04 LTS**.
 - **Instance Type:** `t2.micro` (Free Tier Eligible).
 - **Key Pair:** Create or use an existing key pair.
 - **Security Group:**
 - Allow **HTTP (Port 80)** from 0.0.0.0/0.
 - Allow **SSH (Port 22)** from your IP.
3. **Launch the Instance.**

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

ubuntu

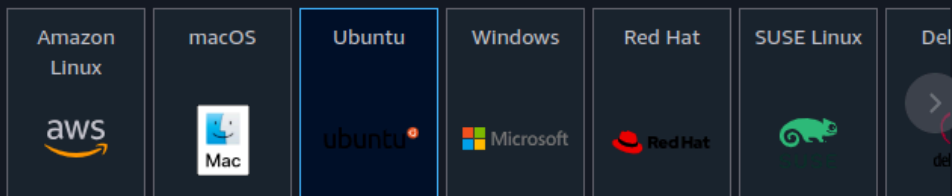
[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

🔍 Search our full catalog including 1000s of application and OS Images

Quick Start



[Browse more AMIs](#)

Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-04dd23e62ed049936 (64-bit (x86)) / ami-0c65913e98a358f43 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible



Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture

64-bit (x86)

AMI ID

ami-
04dd23e62ed049
936

Username

ubuntu



Verified provider

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Linux base pricing: 0.0116 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand RHEL base pricing: 0.026 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

☐ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-07fecafc317c1a7da
172.31.0.0/16

(default)



Subnet [Info](#)

subnet-0c7ebe01854ca2dc9

VPC: vpc-07fecafc317c1a7da Owner: 953065575275

Availability Zone: us-west-2a Zone type: Availability Zone

IP addresses available: 4091 CIDR: 172.31.16.0/20



[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable



Additional charges apply when outside of **free tier allowance**

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

Security group name - *required*

ubuntu-sg

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, and ._-:/()#,@[]+=&:!\$*

Inbound Security Group Rules

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

Type	Protocol	Port range
ssh	TCP	22

Source type	Source	Description - optional
Anywhere	<input type="text" value="Add CIDR, prefix list or security gr..."/> 0.0.0.0/0	e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0) Remove

Type	Protocol	Port range
HTTP	TCP	80

Source type	Source	Description - optional
Custom	<input type="text" value="Add CIDR, prefix list or security gr..."/> 0.0.0.0/0	e.g. SSH for admin desktop

Rules with source of 0.0.0.0/0 allow all IP addresses to access your Instance. We recommend setting security

▼ Configure storage Info Advanced

1x GiB Root volume (Not encrypted)

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

Add new volume

The selected AMI contains more instance store volumes than the Instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the Instance

☐ Click refresh to view backup information

The tags that you assign determine whether the Instance will be backed up by any Data Lifecycle Manager policies.

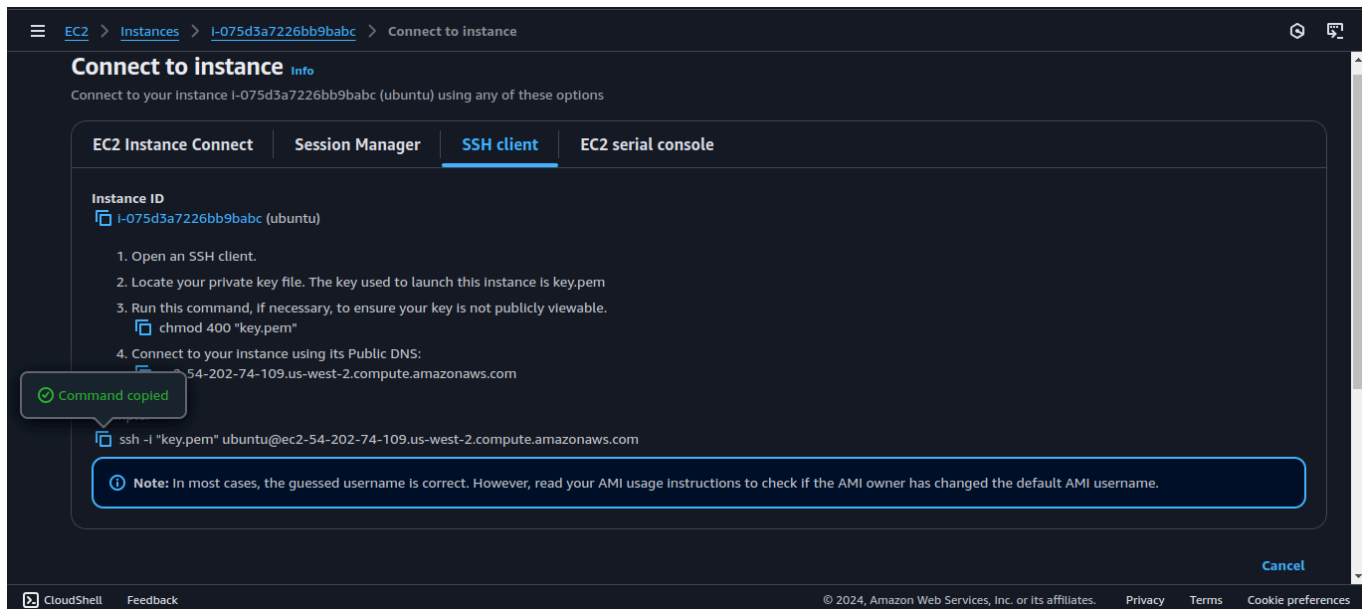
0 x File systems Edit

► Advanced details Info

Step 2: Connect to the EC2 Instance

- 1. Use SSH to connect:

```
ssh -i "your-key-file.pem" ubuntu@<INSTANCE_PUBLIC_IP>
```



EC2 > Instances > i-075d3a7226bb9babc > Connect to instance

Connect to instance Info

Connect to your instance i-075d3a7226bb9babc (ubuntu) using any of these options

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

Instance ID
i-075d3a7226bb9babc (ubuntu)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is key.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
`chmod 400 "key.pem"`
4. Connect to your instance using its Public DNS:
ec2-54-202-74-109.us-west-2.compute.amazonaws.com

Command copied

```
ssh -i "key.pem" ubuntu@ec2-54-202-74-109.us-west-2.compute.amazonaws.com
```

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```
System information as of Thu Nov 28 17:29:23 UTC 2024

System load:  0.19           Processes:            106
Usage of /:   22.9% of 6.71GB Users logged in:           0
Memory usage: 21%           IPv4 address for enX0: 172.31.18.157
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-172-31-18-157:~$
```

1. Update the System:

```
sudo apt update
sudo apt upgrade -y
```

```
ubuntu@ip-172-31-18-157:~$ sudo apt update
Hit:1 http://us-west-2.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://us-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://us-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://us-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:8 http://us-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:9 http://us-west-2.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:10 http://us-west-2.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
```

```
ubuntu@ip-172-31-18-157:~$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
#
# Patches available for the local privilege escalation issue in needrestart
# tracked by CVE-2024-48990, CVE-2024-48991, CVE-2024-48992, and CVE-2024-10224
# For more see: https://ubuntu.com/blog/needrestart-local-privilege-escalation
#
The following NEW packages will be installed:
  linux-aws-headers-6.8.0-1019 linux-aws-tools-6.8.0-1019 linux-headers-6.8.0-1019-aws linux-image-6.8.0-1019-aws
```

Step 3: Install Apache Web Server

1. Install Apache:

```
sudo apt install apache2 -y
```

```
ubuntu@ip-172-31-18-157:~$ sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
```

2. Start and Enable Apache:

```
sudo systemctl start apache2
sudo systemctl enable apache2
```

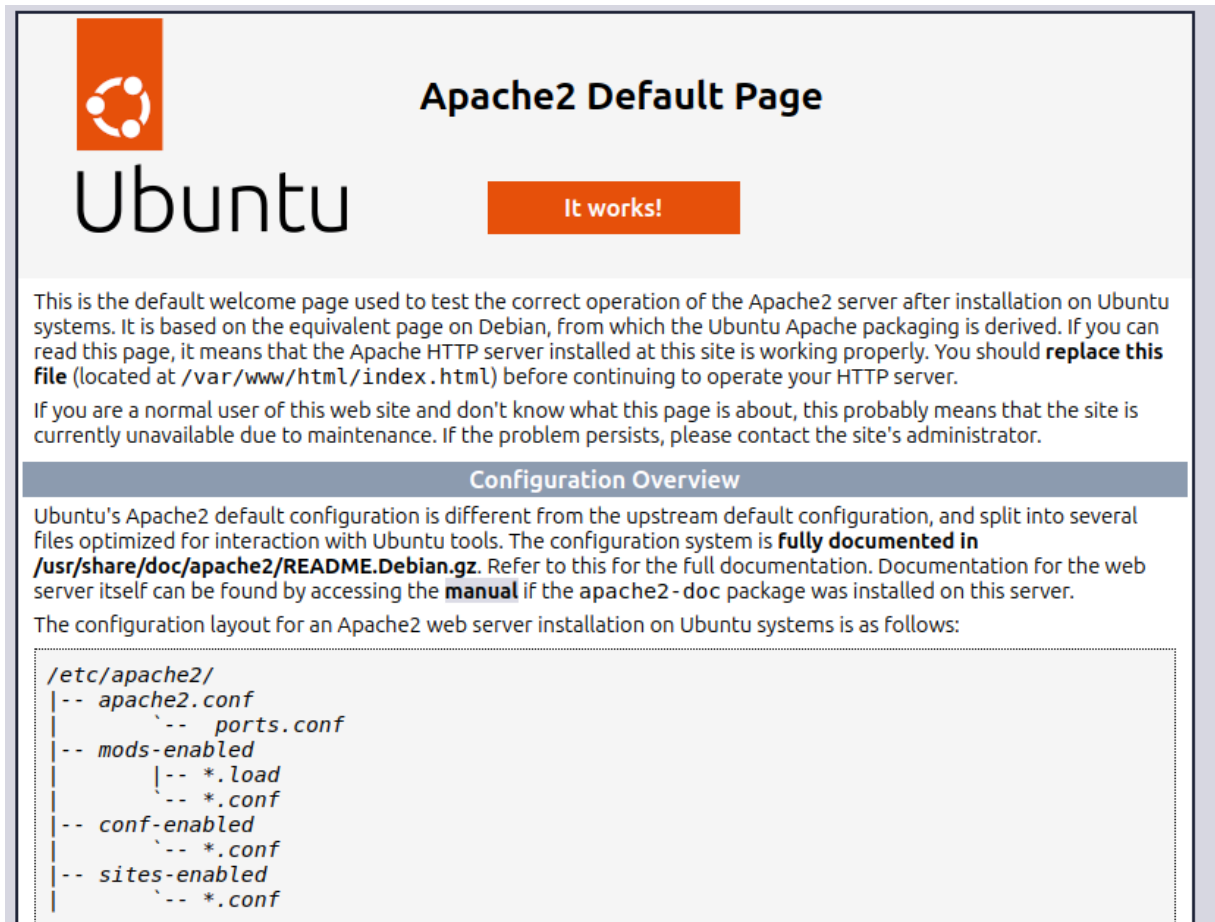
```
ubuntu@ip-172-31-18-157:~$ sudo systemctl start apache2
sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
```

3. Verify Apache:

- Open a browser and visit:

http://<INSTANCE_PUBLIC_IP>

- You should see the Apache default page.



Step 4: Create the HTML/CSS Web Page

1. Write the HTML File:

- Create a new file:

```
```bash
sudo vi /var/www/html/index.html
```

![[14-vi 2.png]]
```

- Add the following content:

```
```html
<!DOCTYPE html>
```

# Welcome to My Test Website!

This is a simple webpage to test your Apache server.

Enjoy testing!

```
```
```

```
![[15-vi.png]]
```

2. Save the File:

- Press `:`, then `X` to save and exit.

Step 5: Test the Web Page

1. Open your browser and visit:

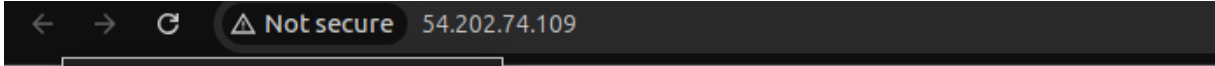
```
http://<INSTANCE_PUBLIC_IP>
```

2. You should see the webpage with the following:

- A header with the title "Welcome to My Test Website!."
- A main section with the message:

This is a simple webpage to test your Apache server.

Enjoy testing!



Click to go back, hold to see history

Welcome to My Test Website!

This is a simple webpage to test your Apache server.

Enjoy testing!

Step 6: Secure and Clean Up

1. Restrict SSH Access:

- Update the security group to allow SSH only from your IP.

2. Clean Up Files (Optional):

- Remove unnecessary default files in `/var/www/html`:

```
sudo rm /var/www/html/index.html.bak
```