

Screenshot of the AWS EC2 'Launch an instance' wizard.

Step 1: Name and tags

- Name: Windows-Webserver
- Add additional tags

Step 2: Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search: Search our full catalog including 1000s of application and OS images

Recent AMIs: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian

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

Step 3: Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.10... [read more](#)
ami-07ff62358b87c7116

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

Cancel | Launch instance | Preview code

Step 4: Amazon Machine Image (AMI) details

Microsoft Windows Server 2022 Base
ami-0fc8a85749a35ce56 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description: Microsoft Windows Server 2022 Datacenter edition. [English]

Architecture: 64-bit (x86) | AMI ID: ami-0fc8a85749a35ce56 | Publish Date: 2025-12-10 | Username: Administrator | Verified provider

Step 5: Instance type

t2.micro (Family T2, 1 vCPU, 1 GiB Memory, Current generation: true)
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour | On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

Additional costs apply for AMIs with pre-installed software

All generations | Compare instance types

Step 6: Summary (continued)

Number of instances: 1

Software Image (AMI): Microsoft Windows Server 2022 ... [read more](#)
ami-0fc8a85749a35ce56

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 30 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

Cancel | Launch instance | Preview code

T2.micro is not available in 2025 Microsoft windows so we use 2022 version

Screenshot of the AWS EC2 'Launch an Instance' wizard, Step 2: Set instance details.

Key pair (login)

You can use a key pair to securely connect to your instance. Ensure you have a key pair ready to use.

Key pair name - required

Select **lokeskey**

For Windows instances, you use a key pair to decrypt the administrator password.

Network settings

Network: vpc-09f65927430f07f67

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enabled

Additional charges apply when outside of free tier allowance

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance.

Create security group

We'll create a new security group called 'launch-wizard-3' with the following rules:

Allow RDP traffic from Anywhere

Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

Create key pair

Key pair name: lokeskey

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA RSA encrypted private and public key pair

ED25519 ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

.pem For use with OpenSSH

.ppk For use with PuTTY

When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more ↗

Summary

Number of instances: 1

Software Image (AMI): Microsoft Windows Server 2022 ...read more

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 30 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

Launch instance

Screenshot of the AWS EC2 'Launch an Instance' wizard, Step 2: Set instance details.

Network settings

Network: vpc-09f65927430f07f67

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enabled

Additional charges apply when outside of free tier allowance

Firewall (security groups)

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

We'll create a new security group called 'launch-wizard-3' with the following rules:

Allow RDP traffic from Anywhere

Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Summary

Number of instances: 1

Software Image (AMI): Microsoft Windows Server 2022 ...read more

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 30 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

Launch instance

Screenshot of the AWS EC2 'Launch an instance' wizard.

Configure storage:

- Root volume: 30 GiB gp2
- Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage.
- Add new volume

Advanced details:

- AMI: Microsoft Windows Server 2022
- Virtual server type: t2.micro
- Firewall: New security group
- Storage: 1 volume(s) - 30 GiB

Summary:

- Number of instances: 1
- Software Image (AMI): Microsoft Windows Server 2022
- Virtual server type (instance type): t2.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 30 GiB

Actions:

- Cancel
- Launch instance
- Preview code

Screenshot of the AWS EC2 instance details page for i-0a745fa5e6907684e.

Session Manager:

- Record RDP connections: You can now record RDP connections using AWS Systems Manager just-in-time node access. [Learn more](#)
- Try for free

Connection Type:

- Connect using RDP client: Download a file to use with your RDP client and retrieve your password.
- Connect using Fleet Manager: To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#).

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following username and password:

Public DNS: ec2-5-93-187-44.compute-1.amazonaws.com

Username: Administrator

Password: Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Actions:

- CloudShell
- Feedback
- Console Mobile App
- © 2026, Amazon Web Services, Inc. or its affiliates.
- Privacy
- Terms
- Cookie preferences

Screenshot of the AWS CloudShell interface showing the "Get Windows password" step for an EC2 instance.

Instance ID: i-0a745fa5e6907684e (Windows-Webserver)

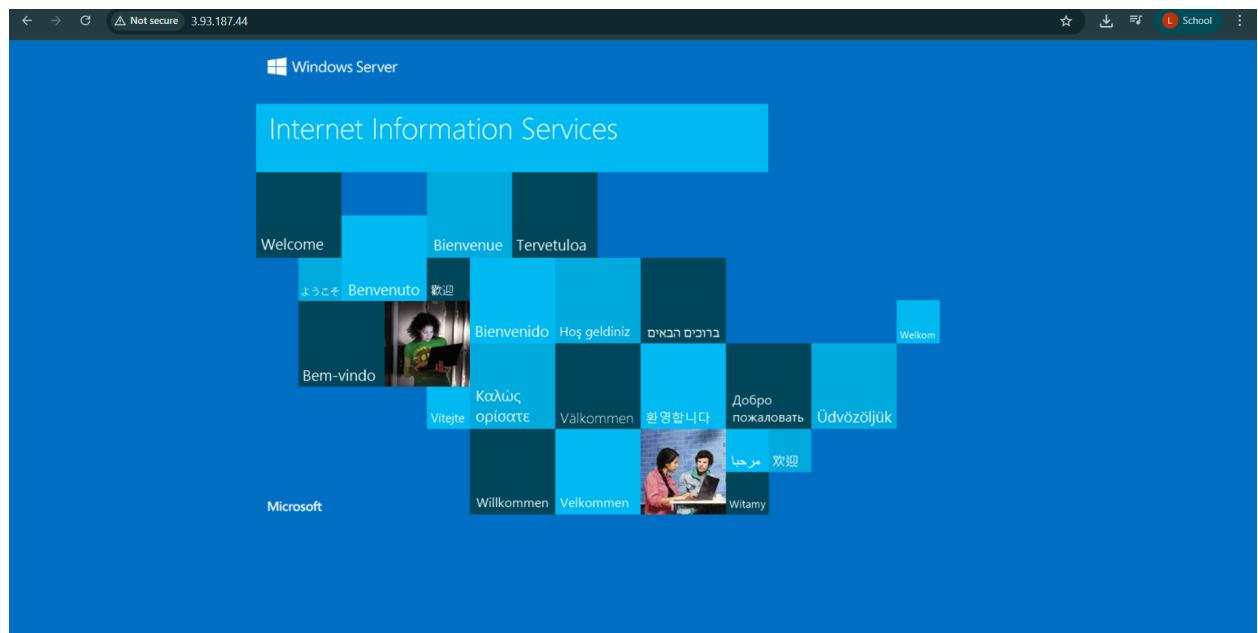
Key pair associated with this instance: lokesthkey

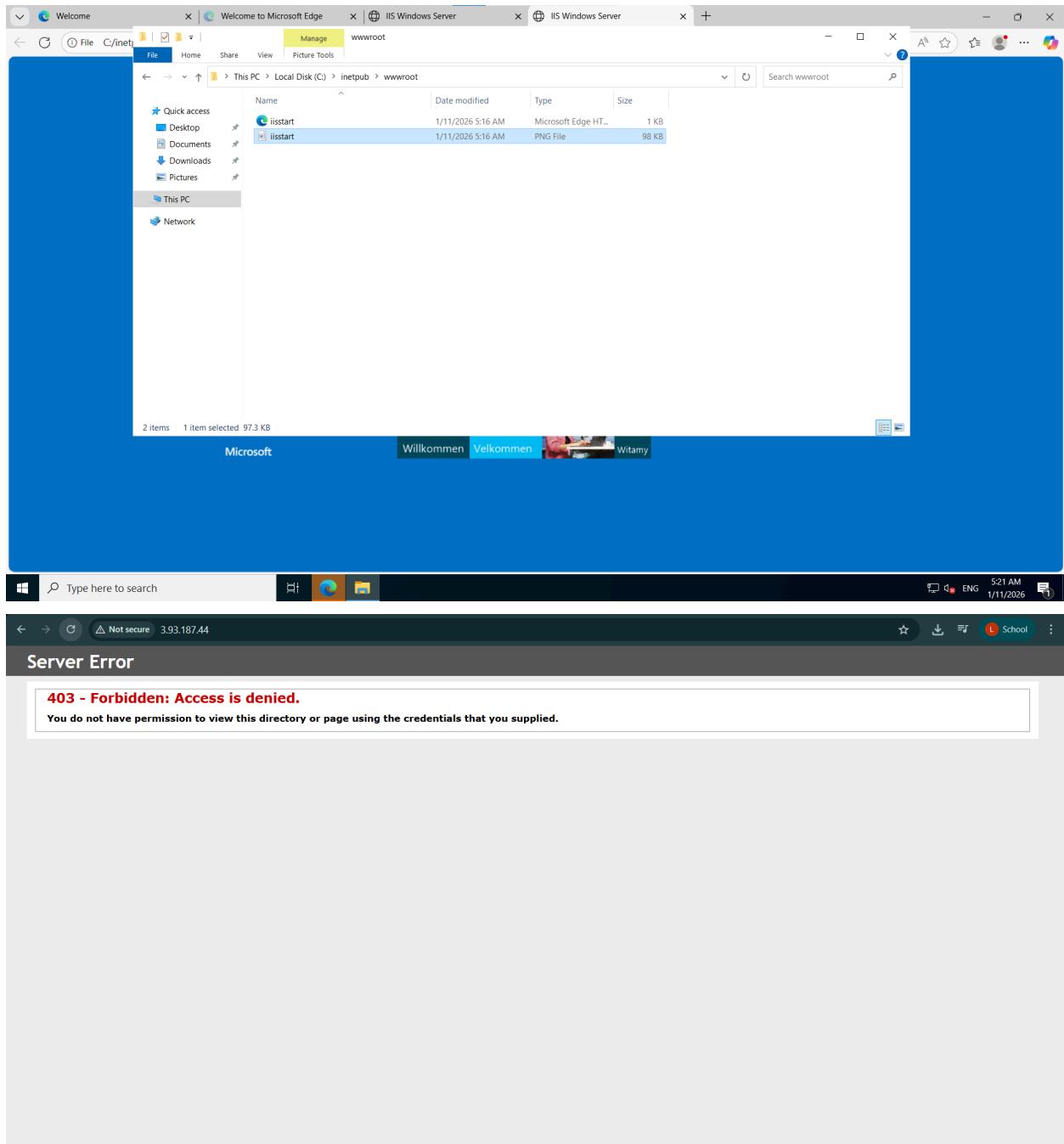
Private key: (Upload private key file)

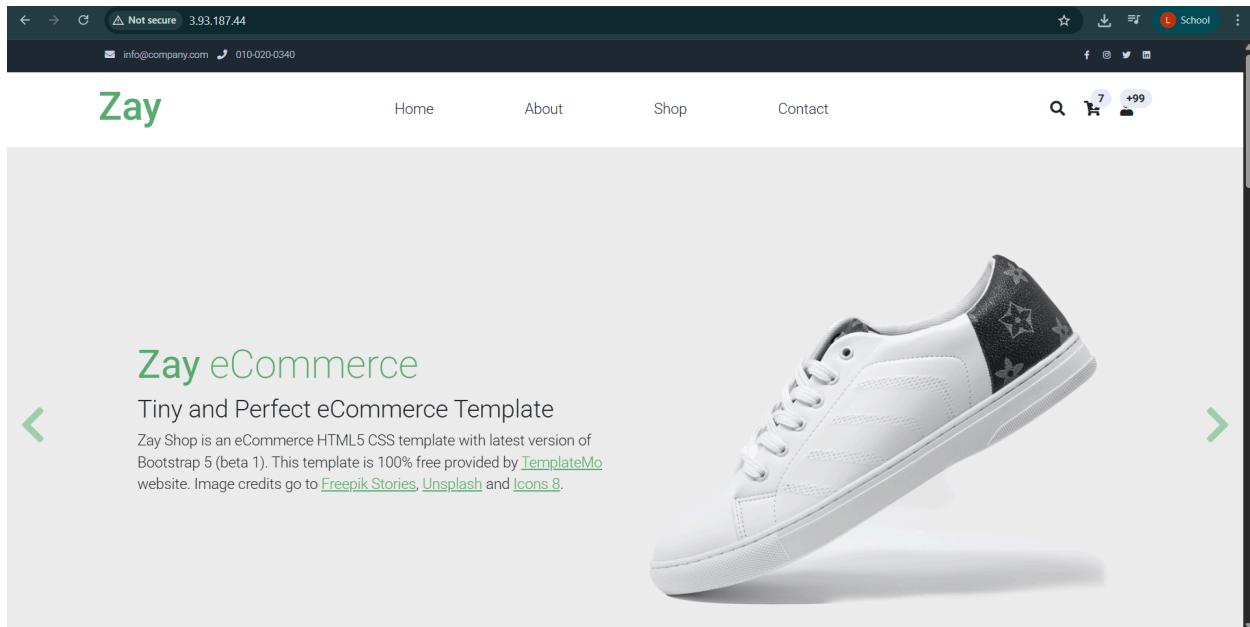
Private key contents:

```
Private key contents
```

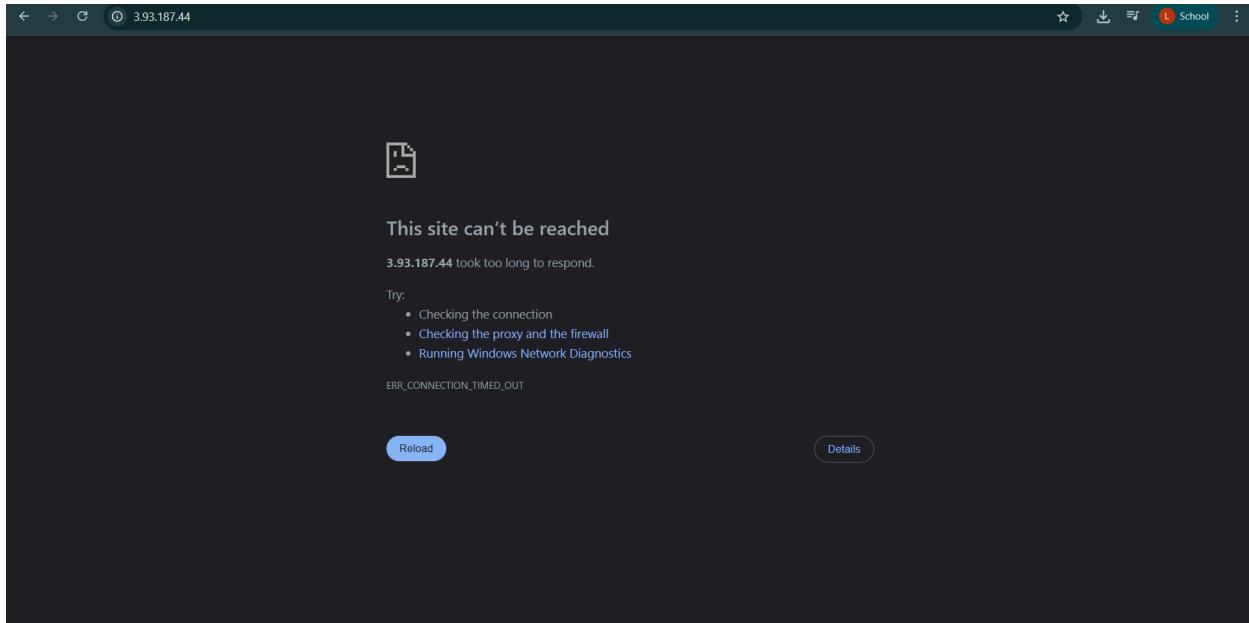
Buttons: Cancel, Decrypt password







A screenshot of the AWS Management Console showing the EC2 Instances page. The left sidebar shows the navigation path: EC2 > Instances. The main content area displays a table of instances. A green banner at the top indicates that the instance 'i-0a745fa5e6907684e' has been successfully terminated. The table shows one instance named 'Windows-Web...' with Instance ID 'i-0a745fa5e6907684e', Instance state 'Terminated', Instance type 't2.micro', and Availability Zone 'us-east-1b'. The 'Details' tab is selected in the instance summary section, which provides information about the instance ID, IPv6 address, and hostname type.



Now we will create a Linux EC2 and Host the same website which is static

Here we chosen Amazon Linux

As this is Linux machine enable SSH if windows we would do RDP

Enable HTTP traffic so that we can hit and see the output of website

Only enabling leads to access the website.

But we will not enable now for learning we will do by not enabling and see the error (not accessing) and then we will enable and check whether we can access the website after enabling

Screenshot of the AWS EC2 Instances page showing two running instances: Linux-Webserver (i-0cb14ec46cdfd87c9) and Windows-Web... (i-0a745fa5e6907684e). The Linux instance is selected.

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
Linux-Webserver	i-0cb14ec46cdfd87c9	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	ec2-98-84-1
Windows-Web...	i-0a745fa5e6907684e	Terminated	t2.micro	-	View alarms +	us-east-1b	-

i-0cb14ec46cdfd87c9 (Linux-Webserver)

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

Instance summary

Instance ID i-0cb14ec46cdfd87c9	Public IPv4 address 98.84.100.132 open address ↗	Private IPv4 addresses 172.31.16.228
IPv6 address -	Instance state Running	Public DNS ec2-98-84-100-132.compute-1.amazonaws.com open address ↗

PutTY Configuration

Category: Session

Basic options for your PuTTY session

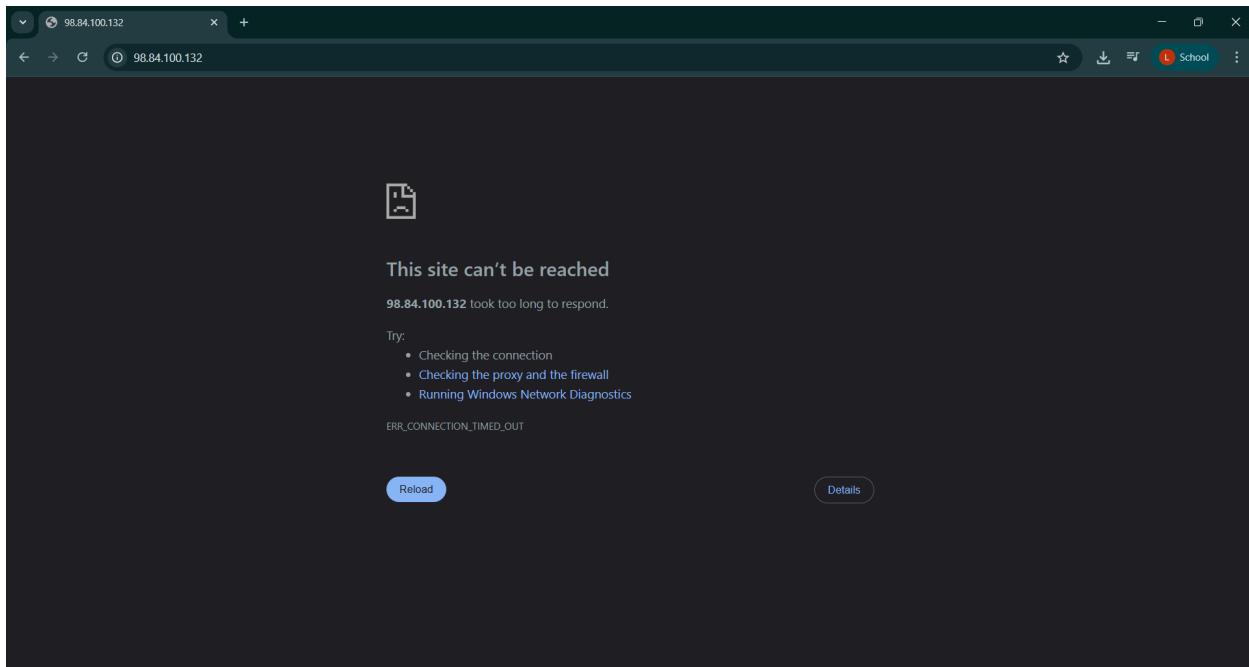
- Specify the destination you want to connect to:
 - Host Name (or IP address): 98.84.100.132
 - Port: 22
- Connection type: SSH (selected)
- Load, save or delete a stored session:
 - Default Settings
 - Load
 - Save
 - Delete
- Close window on exit:
 - Always
 - Never
 - Only on clean exit (selected)

Tags

Private IPv4 addresses
172.31.16.228

Public DNS
ec2-98-84-100-132.compute-1.amazonaws.com

And upload the .ppk file



As we are using nginx we need to see the nginx page but we seeing the site can't be reached error.

Because we not enabled HTTP.

So we need to enable the inbound access to HTTP

A screenshot of the AWS EC2 Instances details page. The instance ID is i-0cb14ec46cdfd87c9. The 'Security' tab is selected. Under 'Security details', it shows the IAM Role (empty), Owner ID (057569470265), and Launch time (Sun Jan 11 2026 11:08:32 GMT+0530 (India Standard Time)). Under 'Inbound rules', there is one rule: Name: -, Security group rule ID: sgr-01d3b6c200110a5f6, Port range: 22, Protocol: TCP, Source: 0.0.0.0/0, and Security groups: launch-wizard-4. Under 'Outbound rules', there is one rule: Name: -, Security group rule ID: rgr-027e110a5f02a722aa, Port range: All, Protocol: All, Destination: 0.0.0.0/0, and Security groups: launch-wizard-4. The left sidebar shows navigation links for EC2, Instances, Images, and Elastic Block Store.

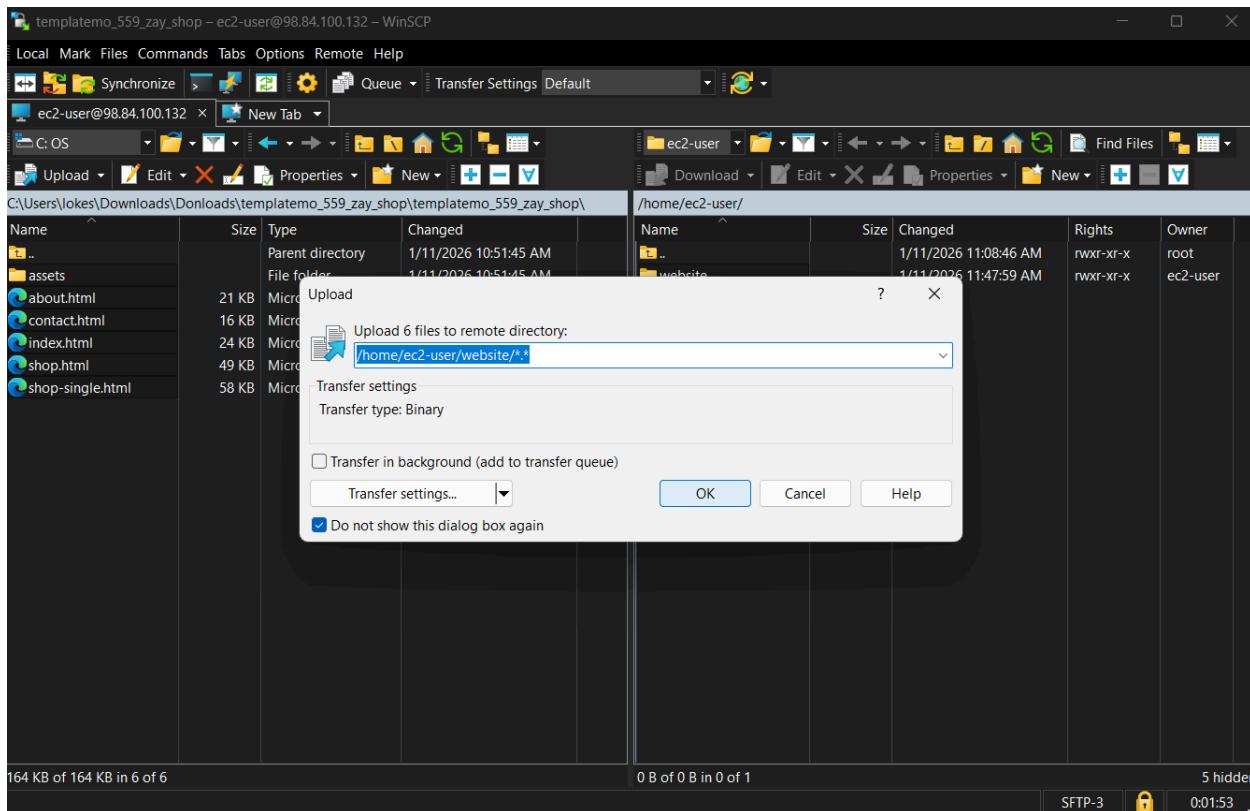


Hello World!

This is a paragraph of text.

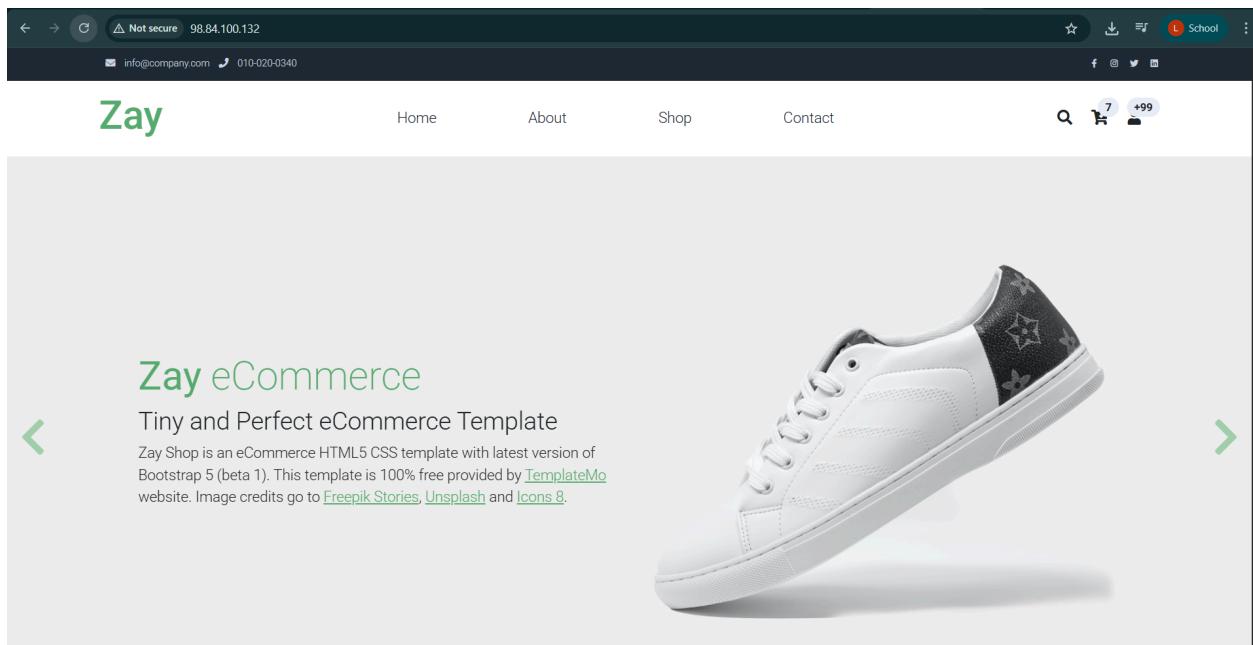
Even after allowing HTTP in security group we faced issue like not getting output because

Systemctl status nginx is not active



For custom page we need to display we using tool called WinScp
In WinScp we need to give our IP address and .PPK key file and we can copy all

```
[root@ip-172-31-16-228:var/www/html
website
[ec2-user@ip-172-31-16-228 ~]$ cd website
[ec2-user@ip-172-31-16-228 website]$ ls
assets
[ec2-user@ip-172-31-16-228 website]$ ls
about.html assets contact.html index.html shop-single.html shop.html
[ec2-user@ip-172-31-16-228 website]$ sudo su - root
Last login: Sun Jan 11 06:01:28 UTC 2026 on pts/3
[root@ip-172-31-16-228 ~]# ls
[root@ip-172-31-16-228 ~]# cd /var/www/html
[root@ip-172-31-16-228 html]$ ls
index.html
[root@ip-172-31-16-228 html]$ rm index.html
rm: remove regular file 'index.html'? y
[root@ip-172-31-16-228 html]$ ls
[root@ip-172-31-16-228 html]$ cp /home/ec2-user/website/* /var/www/html/
cp: -r not specified; omitting directory '/home/ec2-user/website/assets'
[root@ip-172-31-16-228 html]$ cp -r /home/ec2-user/website/* /var/www/html/
cp: overwrite '/var/www/html/about.html'? y
cp: overwrite '/var/www/html/contact.html'? y
cp: overwrite '/var/www/html/index.html'? y
cp: overwrite '/var/www/html/shop-single.html'? y
cp: overwrite '/var/www/html/shop.html'? y
[root@ip-172-31-16-228 html]#
```



See we hosted same in linux machine

Not secure 98.84.100.132/contact.html

info@company.com 010-020-0340

Zay Home About Shop Contact

7 +99

Contact Us

Proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet.

Zay eCommerce Template Location.

Leaflet | Zay Template | Template Design by Templatemo | Map data © OpenStreetMap contributors, CC-BY-SA, Imagery © Mapbox

A screenshot of a web browser displaying a contact page for an eCommerce template named "Zay". The page features a header with navigation links for Home, About, Shop, and Contact, along with social media icons and a search bar. The main content area has a light gray background with a central heading "Contact Us" and a paragraph of placeholder text. Below this is a map interface with a single blue location pin. A tooltip above the pin reads "Zay eCommerce Template Location.". In the bottom right corner of the map area, there is small text indicating the map's source and contributors. The browser's address bar shows the URL "98.84.100.132/contact.html" and indicates the connection is "Not secure". The status bar at the bottom of the browser window shows the IP address "98.84.100.132", the port "010-020-0340", and the email "info@company.com".