

Sandbox Project: Deploying a Webpage in a Windows Server

Objectives:

Create a windows server using AWS Ec2 instance.

Deploy a simple webpage/website in the server.

Scope:

Using sandbox environment.

Launching Ec2 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

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) Info

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](#).

Quick Start

[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

[Microsoft Windows Server 2025 Base](#)

ami-0effe5160a1079475 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

[Free tier eligible](#)

▼ Instance type Info | Get advice

Instance type

[t3.medium](#)

Family: t3 2 vCPU 4 GiB Memory Current generation: true
On-Demand SUSE base pricing: 0.0979 USD per Hour
On-Demand Windows base pricing: 0.06 USD per Hour
On-Demand Linux base pricing: 0.0416 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0451 USD per Hour
On-Demand RHEL base pricing: 0.0704 USD per Hour

 All generations[Compare instance types](#)

[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

[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.

▼ Network settings Info

VPC - required Info

(default) 

Subnet Info

[Create new subnet](#)

Availability Zone Info

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

Security group name - required
launch-wizard-1

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

Description - required | [Info](#)
launch-wizard-1 created 2025-08-21T12:38:06.333Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 3389, 0.0.0.0/0) [Remove](#)

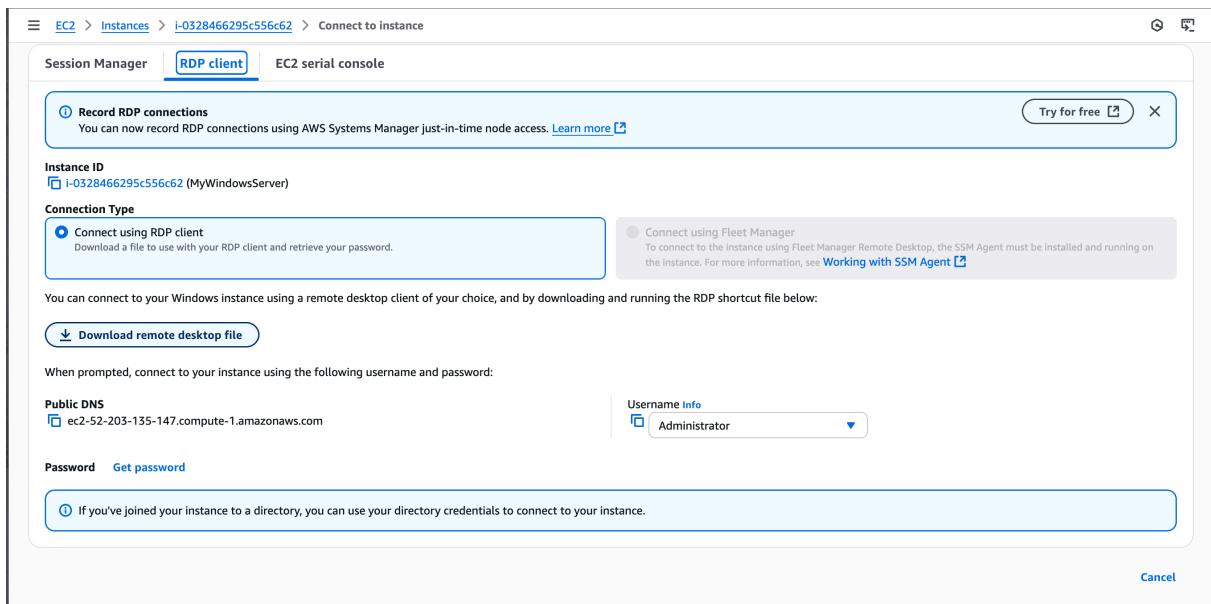
Type Info <input type="radio"/> rdp	Protocol Info <input type="radio"/> TCP	Port range Info 3389
Source type Info <input type="radio"/> Anywhere	Source Info <input type="text"/> Add CIDR, prefix list or security group 0.0.0.0/0 X	Description - optional Info e.g. SSH for admin desktop

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

Type Info <input type="radio"/> HTTP	Protocol Info <input type="radio"/> TCP	Port range Info 80
Source type Info <input type="radio"/> Anywhere	Source Info <input type="text"/> Add CIDR, prefix list or security group 0.0.0.0/0 X	Description - optional Info 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 group rules to allow access from known IP addresses only. X

Connect to the instance using RDP client



Download the RDP file

then click on "Get Password", upload the .pem file that was created/used

Get Windows password Info

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID

i-0328466295c556c62 (MyWindowsServer)

Key pair associated with this instance

vockey

Private key

Either upload your private key file or copy and paste its contents into the field below.

labsuser.pem

1.678KB

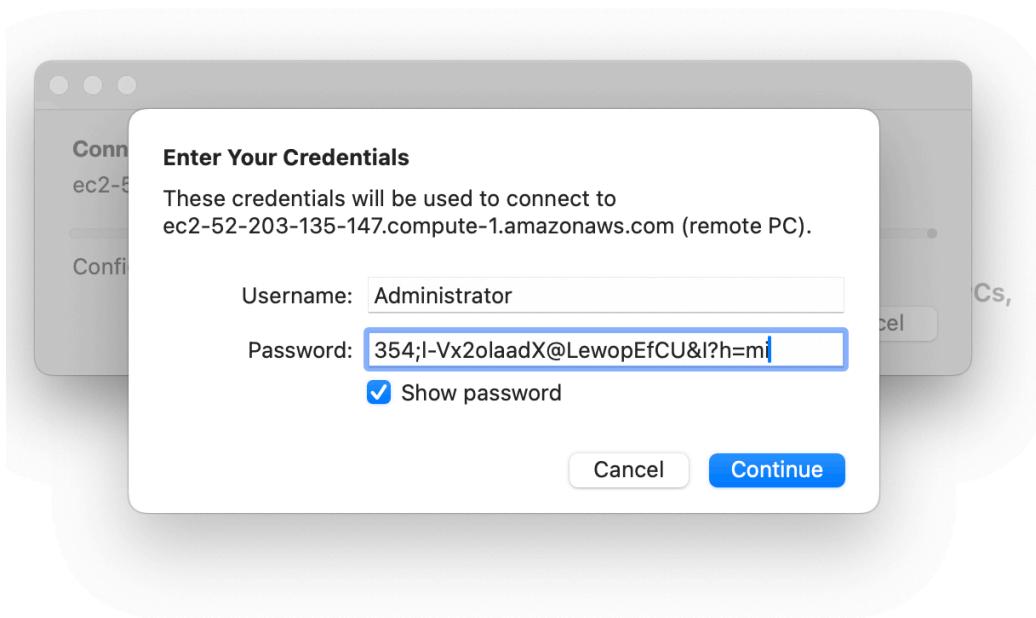
Private key contents - *optional*

-----BEGIN RSA PRIVATE KEY-----

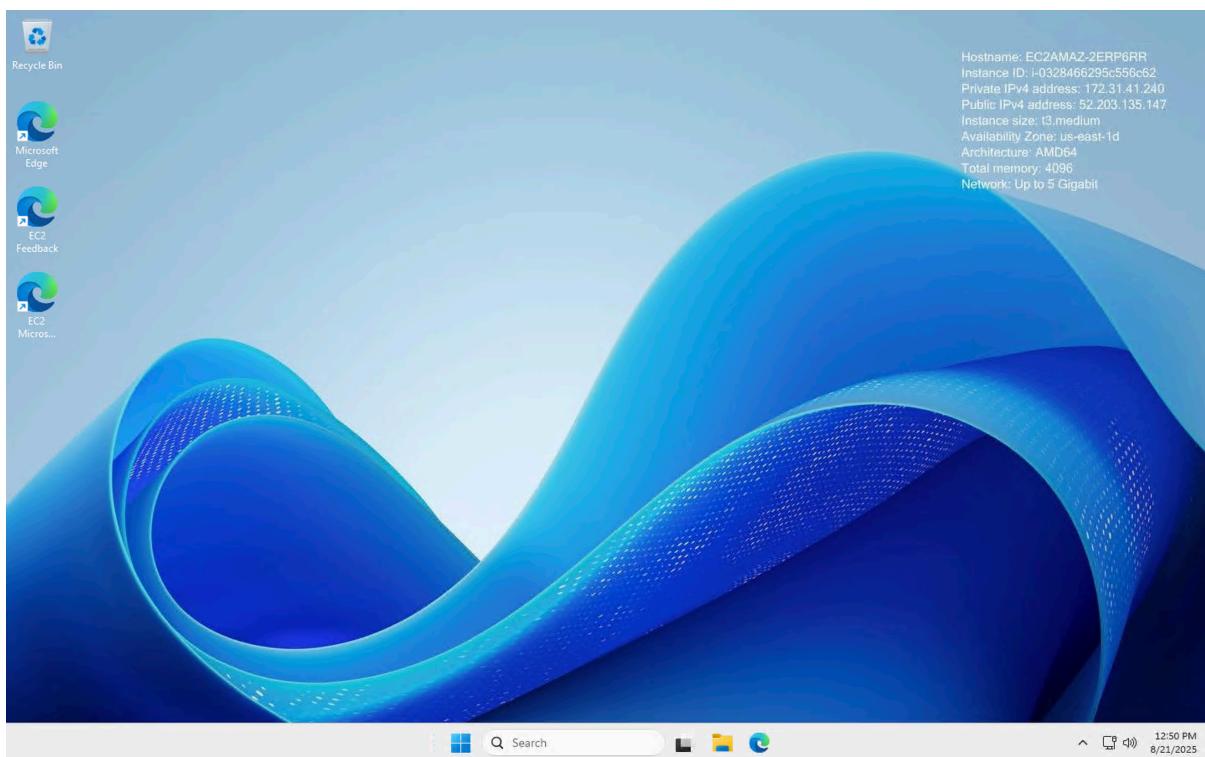
```
MIIEpQIBAAKCAQEA+DnAKrK3/Olvl8xz1qF/LA9sR/5b54Ub2nX0TrkHXNh7QOFq
+f0Qq1yggzt7G2JJHRZlsb5Sk+osJsm3h+qlau36h9ncmOpwYh+uuK+KncpCGDaD
MAZOnZJFC8ksBd2S2mGAHhKe0q8k+P7lj4bVn3fTjraGDAPivswETvOB/jR02zCX
IOM6RXKvHyffhfT8c+oBAP/wxWaZmK17v9VlG+xUlltu2YPBDzZ/2NodJTPNg7vv
LkB36AgFCNk9Vhnb9AK6vgGolh/2gvcEbOfffxomx5WZ/wq79G6it1AhTkMsKUQu
68fRTJFp4OpIn9dGiyzRAnLZkGiKr1xBh9nXQwIDAQABAoIBAAilol8aaLRjgLru
AV8Jsy9qvh/n6XWwOl8q2r7fTTVbyTdiYuKggTMm/+RybBuNRPRUEj3M1M5xh33
```

Decrypt the password and copy it.

open the downloaded RDP file and paste the password there.



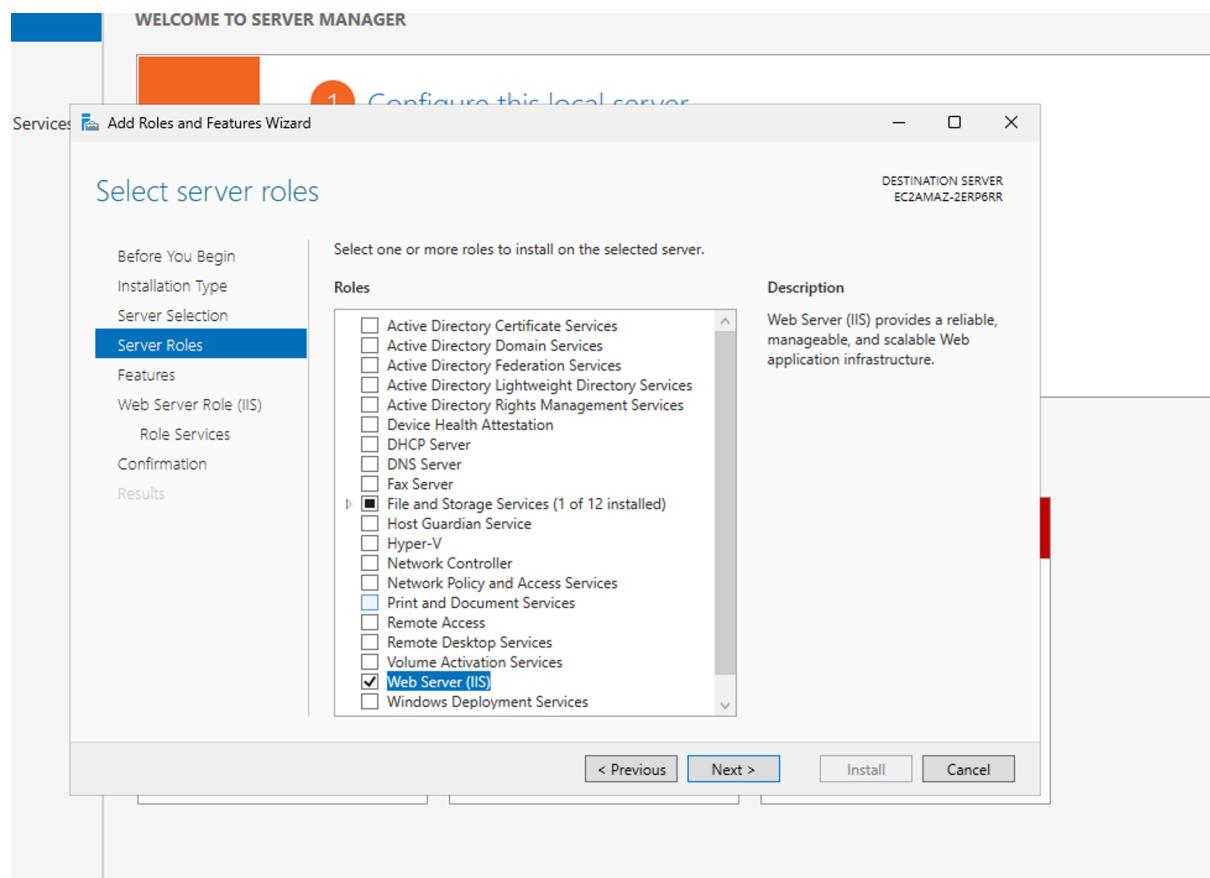
Windows Instance is running



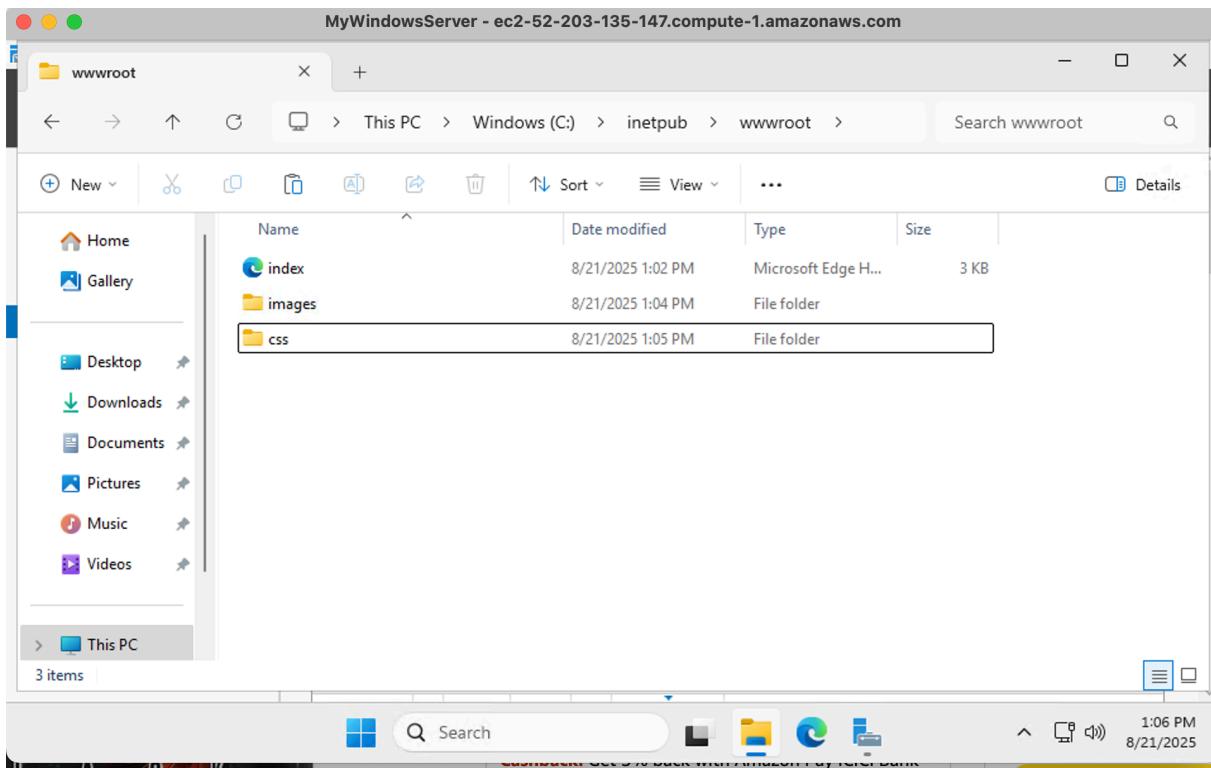
Creating a windows server (IIS)

Just click on IIS in the server roles tab.

Leave everything on default for this tutorial.



Paste your website file in Local Drive (C:) \inetpub\wwwroot



Copy the public IPv4 address of the instance and paste in web browser.

The webpage is now visible.

A screenshot of a Firefox browser window. The address bar shows "Not Secure http://52.203.135.147". The main content area displays a webpage for "Café Al Karim". The page features a header with the text "Café Al Karim" in a stylized font. Below the header are two images: one showing a variety of pastries like croissants and cinnamon rolls, and another showing a display case filled with various cakes and tarts. A descriptive paragraph below the images reads: "The Café offers an assortment of delicious and delectable pastries and coffees that will put a smile on your face. From cookies to croissants, tarts and cakes, each treat is specially prepared to excite your tastebuds and brighten your day!" At the bottom of the page, there are three sections: "Frank bakes a rich variety of cookies. Try them all!", "Tea Coffee Latte Hot Chocolate Yes, we", and "Our tarts are always a customer favorite!". Each section includes an image and some text.