



ELASTIC CLOUD COMPUTE (EC2)

Amazon Elastic Compute Cloud (Amazon EC2) is a web service provided by Amazon Web Services (AWS) that allows users to rent virtual servers in the cloud. EC2 instances provide scalable computing capacity, allowing users to quickly scale up or down based on their application requirements.

Key features of Amazon EC2 include:

1. **Scalability:** Users can easily scale their compute capacity by launching additional instances or stopping unused instances. This flexibility is particularly useful for applications with varying workloads.
2. **Variety of Instance Types:** EC2 offers a wide range of instance types optimized for different use cases, such as compute-optimized, memory-optimized, storage-optimized, and GPU instances.
3. **Customization:** Users can choose the operating system, instance type, storage, and networking configurations for their EC2 instances, providing a high degree of customization to meet specific application requirements.
4. **Security:** EC2 instances can be launched within a Virtual Private Cloud (VPC), allowing users to control network settings, security groups, and access control lists. Amazon EC2 also supports key pairs for secure access to instances.
5. **Pay-as-You-Go Pricing:** Users pay only for the compute capacity they consume, with different pricing options based on instance type, region, and usage duration. This pay-as-you-go model is cost-effective and allows for efficient resource utilization.
6. **Elastic Load Balancing:** EC2 instances can be easily integrated with Elastic Load Balancers to distribute incoming traffic across multiple instances, improving fault tolerance and availability.
7. **AMI (Amazon Machine Image):** Users can create custom machine images containing their applications, configurations, and operating systems, making it easy to launch instances with pre-configured settings.



TO BEGIN WITH LAB:



STEP 1: LAUNCH A WINDOWS EC2 INSTANCE

1. Log in to AWS Console.
2. There you need to search EC2. Choose this service accordingly.



EC2 ☆

Virtual Servers in the Cloud

3. This is the dashboard for EC2. You can find different resources here.

4. But, to create an instance you need to click on **Launch Instance**.

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with various navigation options like Instances, Images, Elastic Block Store, and Network & Security. The main area is titled 'Resources' and shows a summary of Amazon EC2 resources in the Europe (London) Region. It includes tables for Instances (running), Auto Scaling Groups, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, Volumes, and Snapshots. Below this, there's a 'Launch instance' section with a large orange 'Launch instance' button highlighted with a red box. To the right, there's a 'Service health' section and a 'EC2 Free Tier' summary.

5. So, first and foremost, you must name your instance.

The screenshot shows the 'Launch an instance' wizard. The current step is 'Name and tags'. It has a 'Name' input field containing 'WindowsVM' and a 'Add additional tags' link. Above this, there's a general introduction about creating instances in the AWS Cloud.

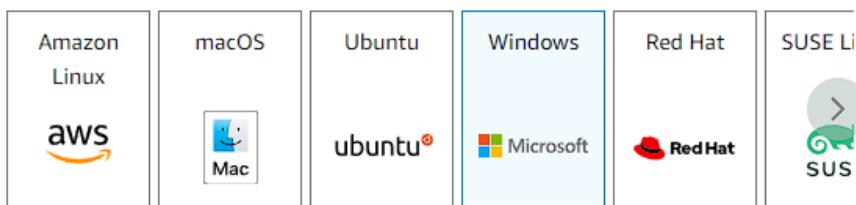
6. Then in the **Application and OS Images**, you have to select an Operating system.
7. Here, you are going to select **Windows** as your Operating system.
8. For **Amazon Machine Image (AMI)**, select the latest AMI that is available. In this case it is Microsoft windows server 2022 base.
9. Keep architecture to default as 64-bit (x86)

▼ 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)

Microsoft Windows Server 2022 Base

ami-088bb7db420bf535c (64-bit (x86))

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

Free tier eligible



Description

Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

Architecture

AMI ID

64-bit (x86)

ami-088bb7db420bf535c

Verified provider

10. Now you must choose an instance type. There are more instance types with higher specifications available, but for the time being, you must select **t2.micro**. This instance type is qualified for the free tier.

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

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0178 USD per Hour
On-Demand RHEL base pricing: 0.0732 USD per Hour
On-Demand SUSE base pricing: 0.0132 USD per Hour
On-Demand Linux base pricing: 0.0132 USD per Hour

Free tier eligible

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

11. In the key pair, you have to create a key pair, so that you can log in to your virtual machine. These key pairs are used as keys to log into your VMs.
12. As of now, you might not have any key pairs, so you have to create a key pair.

▼ 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*

Select

 Create new key pair

13. So, click on create new key pair. First you have to name your keypair.
14. Then select the key pair type as RSA.
15. For the private key file format, select **.pem**
16. Now click on create key pair.

Create key pair



Key pair name

Key pairs allow you to connect to your instance securely.

windows-key

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 ↗](#)

Cancel

Create key pair

17. After clicking on the Create Key Pair button, a file should have been downloaded; this file will be utilized throughout this experiment.
18. Here you can see your key pair.

▼ **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*

windows-key

 [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.

19. If you will take a look at network settings, you will see a VPC which is required and it is a default VPC.
20. The subnet has no preference because you haven't given it any.
21. The **auto assign public IP** feature is enabled.

▼ **Network settings** [Info](#)

VPC - *required* | [Info](#)

vpc-037cc333342ffff6f0
172.31.0.0/16

(default) ▾



Subnet | [Info](#)

No preference



 [Create new subnet](#)

Auto-assign public IP | [Info](#)

Enable



22. In the firewall option, you will see that it is creating a new security group, you can change its name and description, but for the time being keep it to default.

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 2024-01-10T16:27:27.542Z

23. And the security group you will see this Inbound security group rules. These Inbound rules are used for virtual machine to log in to different areas of interest. Let it be default too.

Inbound Security Group Rules

The screenshot shows the 'Inbound Security Group Rules' section of the AWS Management Console. It displays a single rule: 'Security group rule 1 (TCP, 3389, 0.0.0.0/0)'. The rule details are as follows:

- Type: rdp
- Protocol: TCP
- Port range: 3389
- Source type: Anywhere
- Source: 0.0.0.0/0
- Description - optional: e.g. SSH for admin desktop

A warning message is present: "⚠️ 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." with a close button (X).

[Add security group rule](#)

24. Now the setup for EC2 instance is completed, you can click on launch instance. This will launch your instance and you will be able to see your instance.



25. You can see that your instance is launched successfully.

26. Now if you will click on this instance id, you will direct towards your instance.



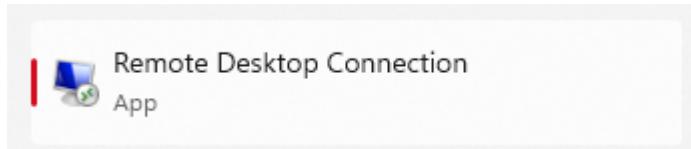
27. Here is your instance, it is up and running.

The screenshot shows the 'Instances (1)' page. The instance details are as follows:

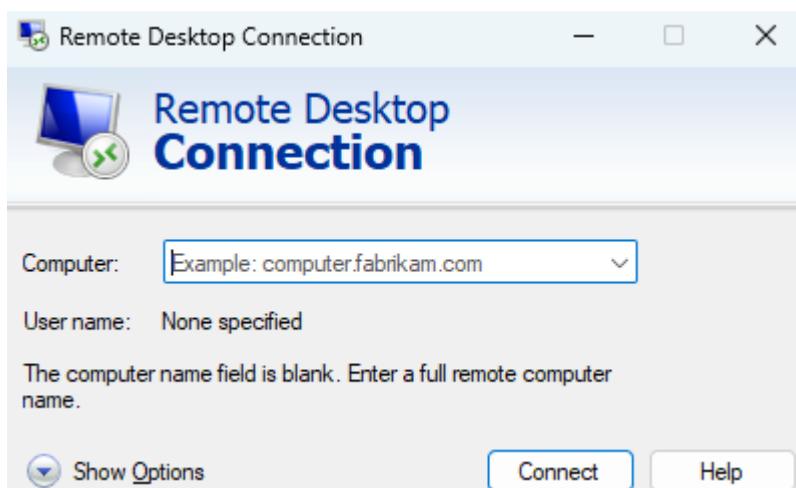
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP
WindowsVM	i-0d5bad9e046098c2c	Running	t2.micro	Initializing	No alarms	eu-west-2b	ec2-35-178-195-66.eu...	35.178.195.66	-

STEP 2: CONNECTING THE INSTANCE

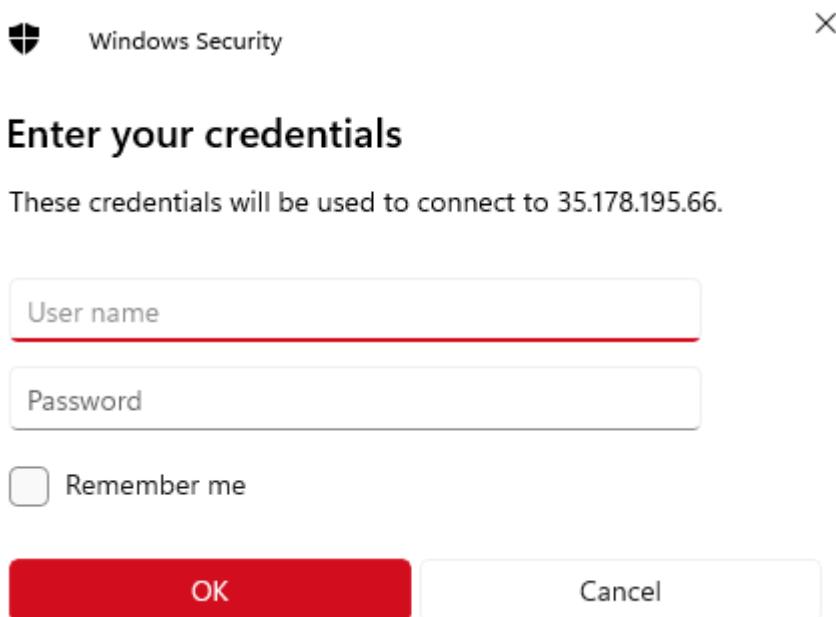
1. So, to connect your windows instance you need to search for RDP (Remote desktop protocol) on your local system. Choose this remote desktop connection accordingly.



2. Now if you click on this, you will see this kind of window has popped up.
3. Here you have to copy the public IP address of your instance, paste it in the computer section. Then click on connect.



4. So, after that the windows security will ask you to enter user name and password.



5. To get your user's name and password you have to come back to the console and click on connect.
6. Here you need to click on RDP client, and you will see bunch of options.
7. You can see your username right there.
8. If you will click on Get Password you can get your password.

The screenshot shows the AWS Session Manager interface with the 'RDP client' tab selected. It displays the following information:

- Instance ID:** i-0d5bad9e046098c2c (WindowsVM)
- Connection Type:**
 - Connect using RDP client:** This option is selected. A tooltip indicates: "Download a file to use with your RDP client and retrieve your password."
 - Connect using Fleet Manager:** A tooltip indicates: "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](#)."
- Public DNS:** ec2-35-178-195-66.eu-west-2.compute.amazonaws.com
- Username:** Administrator
- Password:** [Get password](#)
- Info Message:** "If you've joined your instance to a directory, you can use your directory credentials to connect to your instance."

9. Now you will be directed on a new page to get your password.
10. Here you can see the name of key which is associated with your windows instance.
11. Now you have to upload the .pem file here from your local machine.
12. Once you have uploaded the .pem file, now you have to click on decrypt password.

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

Instance ID

i-0d5bad9e046098c2c (WindowsVM)

Key pair associated with this instance

windows-key

Private key

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

Upload private key file

Private key contents - *optional*

Private key contents

When prompted, connect to your instance using the following details:

Public DNS

ec2-13-40-220-95.eu-west-
2.compute.amazonaws.com

Username

Administrator

Password

;h\$LvywFgxePjP4FWPV?j3z91H-;)yHw

13. Now enter your credentials. Then click on OK.



Enter your credentials

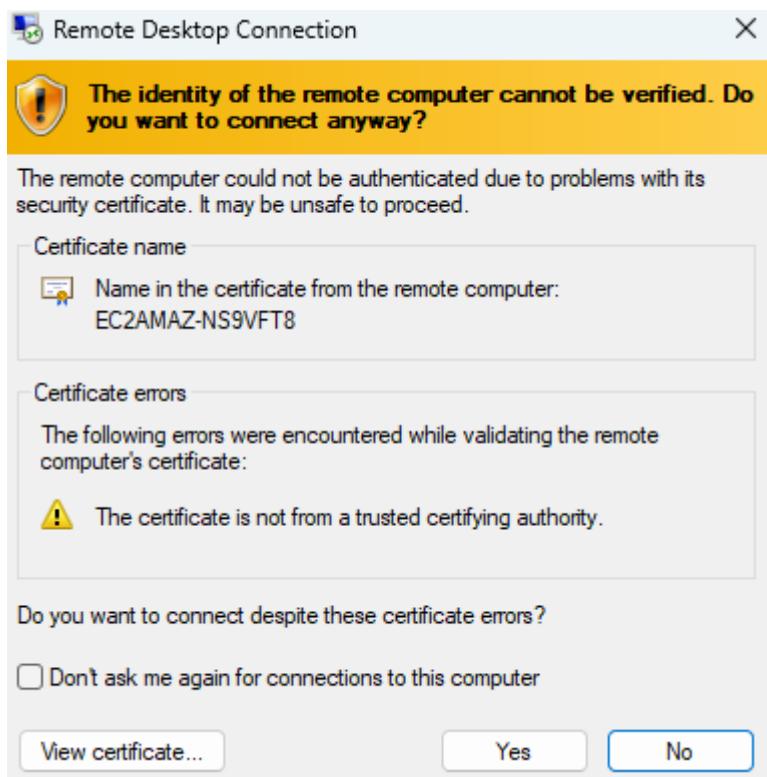
These credentials will be used to connect to 13.40.220.95.

Remember me

OK

Cancel

14. Here also you have click on YES and you will be logged into your windows virtual machine.

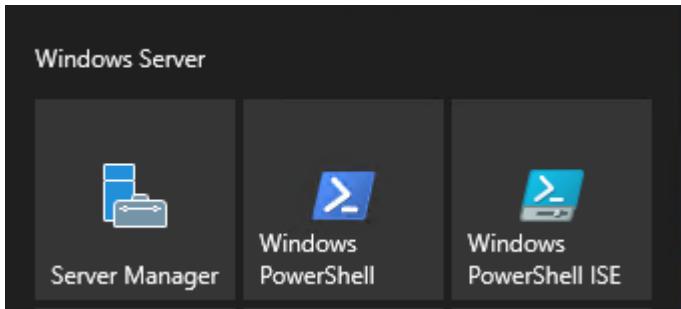


15. Below is your virtual machine for windows instance.

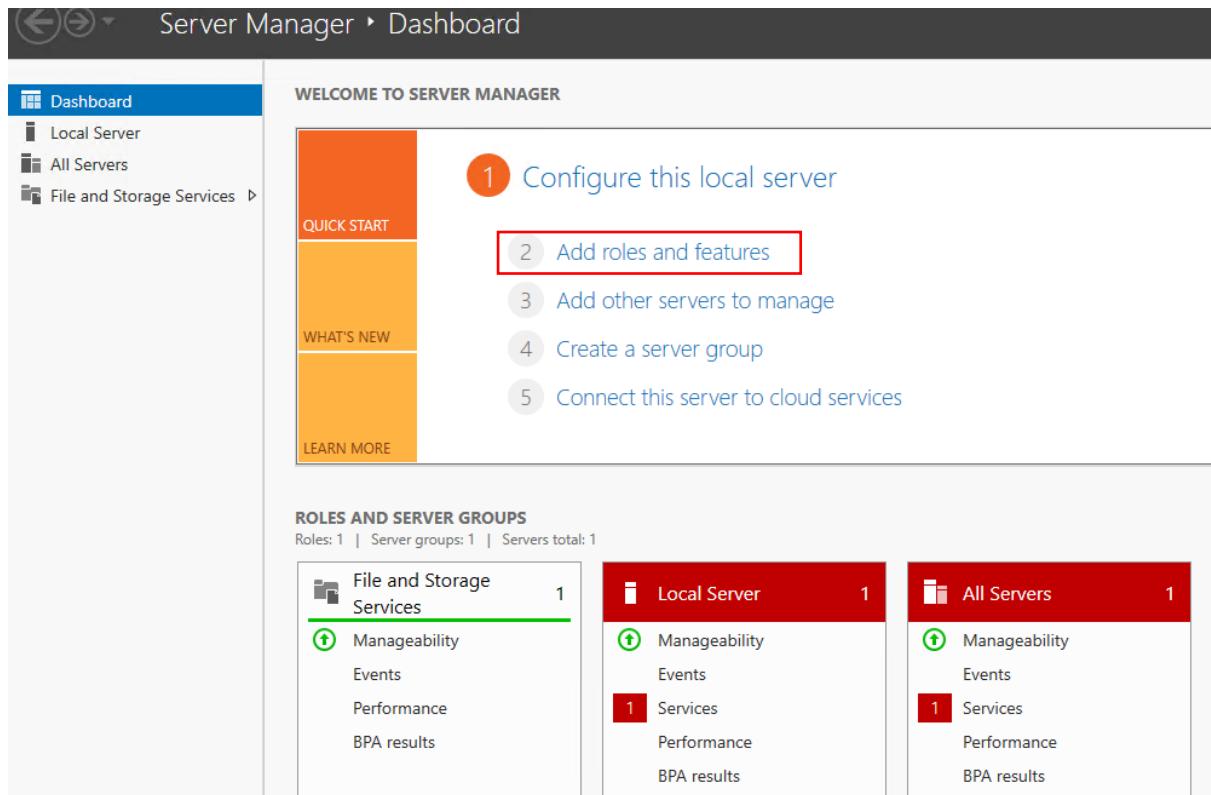


😊 STEP 3: DEPLOYING A WEB SERVER ON THE INSTANCE

1. To deploy the webserver on your virtual machine you need to open **Server Manager**.



2. It might take some time for server manager to setup things.
3. Once your server manager is setup. Now you have to click on **Add roles and features**.



4. Here, you need click on next.

This screenshot shows the 'Before you begin' step of the 'Add Roles and Features Wizard'. The left sidebar lists steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main content area describes the wizard's purpose: to help install roles, role services, or features based on organizational needs like sharing documents or hosting websites. It also provides instructions for removing roles, lists prerequisites (strong password, network settings, security updates), and a note about verifying prerequisites. At the bottom, there's a checkbox for skipping the page and navigation buttons for 'Previous', 'Next >', 'Install', and 'Cancel'.

Before you begin

DESTINATION SERVER
EC2AMAZ-NS9VFT8

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

Skip this page by default

< Previous Next > Install Cancel

5. Then it will ask you to select an installation type choose role based and click on next.

Select installation type

DESTINATION SERVER
EC2AMAZ-NS9VFT8

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

Role-based or feature-based installation

Configure a single server by adding roles, role services, and features.

Remote Desktop Services installation

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel

6. Now it will ask you a destination. Let it be default and click on next.

Select destination server

DESTINATION SERVER
EC2AMAZ-NS9VFT8

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

Select a server from the server pool

Select a virtual hard disk

Server Pool

Filter:		
Name	IP Address	Operating System
EC2AMAZ-NS9VFT8	172.31.34.249	Microsoft Windows Server 2022 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

Cancel

7. Now here you have to select Web server (IIS). This will help you to install the web server on your instance.

Select server roles

DESTINATION SERVER
EC2AMAZ-NS9VFT8

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

Role Services

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services (1 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Controller
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

< Previous

Next >

Install

Cancel

8. Then click on next till you get to the confirmation and now install your web server.

Confirm installation selections

DESTINATION SERVER
EC2AMAZ-NS9VFT8

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

Role Services

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Web Server (IIS)

Web Server

Common HTTP Features

Static Content

Default Document

Directory Browsing

HTTP Errors

Security

Request Filtering

Health and Diagnostics

HTTP

[Export configuration settings](#)

[Specify an alternate source path](#)

< Previous

Next >

Install

Cancel

9. Once your web server is installed come back to the console.

10. So, now you have to add **port 80** to your security group.

11. Now select your instance and go to security, there you will see a link to navigate you to the security group. Click on it.

Instance: i-0bc7f2f0b89682297 (LinuxVM)

Details Security Networking Storage Status checks Monitoring Tags

▼ Security details

IAM Role -

Owner ID 463646775279

Launch time Wed Jan 10 2024 22:22:18 GMT+0530 (India Standard Time)

Security groups

sg-0a32c29b69fd4424f (launch-wizard-1)

12. In the security group you will see some options present over there.

13. If you will just click on edit inbound rules under the inbound rules and add port 80 to your instance.

sg-0a32c29b69fd4424f - launch-wizard-1

Actions ▾

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-1	sg-0a32c29b69fd4424f	launch-wizard-1 created 2024-01-10T16:27:27.542Z	vpc-037cc333342ff6f0
Owner	Inbound rules count	Outbound rules count	
463646775279	1 Permission entry	1 Permission entry	

Inbound rules Outbound rules Tags

Inbound rules (1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-03bf3cb4e17e33d91	IPv4	SSH	TCP	22	0.0.0.0/0	-

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-03bf3cb4e17e33d91	SSH	TCP	22	Custom	0.0.0.0/0 X
-	HTTP	TCP	80	Anywhere...	0.0.0.0/0 X

Add rule

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

Cancel Preview changes Save rules

Inbound rules Outbound rules Tags

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-03bf3cb4e17e33d91	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sgr-083beecd60ba2fc5e2	IPv4	HTTP	TCP	80	0.0.0.0/0	-

14. Now go back to your instance and copy your public IP address and paste it in a new tab.

15. You will see your web server is up and running.

