



AWS Cloud Training

-by Mr.Mahendran Selvakumar

Organized by KPR Institute of Engineering and Technology

Department of Computer Science and Engineering

Name:Sujitha C

II - CSE

A step by step guide on the configuration of Windows web server and access it using public IP address

- Create an Windows EC2 Instance and launch it .

Here are few steps on how to create a Windows EC2 instance and connect from Windows OS

Step 1: Create a name for your instance

The screenshot shows the 'Name and tags' step of the 'Launch an instance' wizard. At the top, there is a breadcrumb navigation: 'EC2 > ... > Launch an instance'. Below the breadcrumb, the section title 'Launch an instance' has an 'Info' link. A descriptive text states: '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.' In the 'Name and tags' section, there is a 'Name' label and a text input field containing 'kprwindows'. To the right of the input field is a blue 'Add additional tags' link.

Step 2 : Choose an AMI from the Windows Section (which is applicable for free tier)

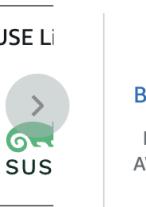
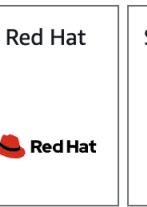
▼ Application and OS Images (Amazon Machine Image) [Info](#)

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*

Recents

Quick Start



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Microsoft Windows Server 2019 Base

ami-021dd3fd9dfffc1699 (64-bit (x86))

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

Free tier eligible



Description

Microsoft Windows 2019 Datacenter edition. [English]

| Architecture | AMI ID | Username | |
|--------------|----------------------------|----------|--------------------------------|
| 64-bit (x86) | ami-021dd3fd9dfffc1 699 | root | Verified provider |

Step 3 :Choose an instance type (which is applicable for free tier) and then name your key pair in the next step

The screenshot shows the 'Instance type' section of the AWS CloudFormation 'Create New Stack' wizard. It lists the 't2.micro' instance type as 'Free tier eligible'. Below the list, it says 'Additional costs apply for AMIs with pre-installed software'. To the right, there are buttons for 'All generations' and 'Compare instance types'. The 'Key pair (login)' section below it shows a dropdown menu with 'kprwindow' selected, and a 'Create new key pair' button.

▼ 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: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand SUSE base pricing: 0.0124 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

kprwindow ▼ [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.

Step 4: Create a new key pair

- Enter the name for your key pair
- Choose the Key pair type as RSA(it is the only option available as you cannot choose ED25519 since it is not available for Windows instances).
- Choose .pem private key file format and click on Create key pair .

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

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](#)

Once you have created the Key pair it will be downloaded to your PC by default .

Step 5: Set the network settings

In the Network Settings the VPC required and all other fields like Subnet , Auto -assign public IP fields are filled by default

▼ Network settings [Info](#)

VPC - required [Info](#)

| | | |
|-----------------------|-------------|-------------------|
| vpc-0be03f8df40a75130 | (default) ▾ | C |
| 172.31.0.0/16 | | |

Subnet [Info](#)

| | | |
|---------------|---|-------------------------------------|
| No preference | ▼ | C Create new subnet |
|---------------|---|-------------------------------------|

Auto-assign public IP [Info](#)

| | |
|--------|---|
| Enable | ▼ |
|--------|---|

Additional charges apply when outside of [free tier allowance](#)

Step 6: Security group

Select Create Security group and provide a name for it

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*
kprwindows

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 2024-10-07T10:20:24.639Z

Inbound Security Group Rules

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

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

⚠ 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

[Add security group rule](#)

The Description required column and the Inbound Security Group Rules are filled by the default values and better not to change it.

Step 7 : Set the Configure Storage (usually it is 30 Gb for Windows and 8 Gb for Linux)

The screenshot shows the 'Configure storage' section of the AWS Lambda setup. It displays a configuration for a single volume: 1x 30 GiB gp2, labeled as a Root volume (Not encrypted). A note indicates that free-tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Below this, a message states that the selected AMI contains more instance store volumes than the instance allows, and only the first 0 instance store volumes from the AMI will be accessible from the instance. A note also mentions that tags assigned to the instance determine backup behavior via Data Lifecycle Manager policies. At the bottom, there is a section for 'File systems' with an 'Edit' button.

After completing all these steps click on Launch instance and open the instances page

Step 8 : Follow the below steps to connect

The screenshot shows the AWS Instances page with one instance listed. The instance is named 'kprwindows', has an ID of 'i-07708cc04eb40d2e0', is in the 'Running' state, and is of type 't2.micro'. It is currently initializing. The page includes filters for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IP, along with a search bar and pagination controls.

Select the instance and click on connect

Connect to Instance Info

Connect to your instance i-07708cc04eb40d2e0 (kprwindows) using any of these options

Session Manager | **RDP client** | EC2 serial console

Instance ID

[i-07708cc04eb40d2e0 \(kprwindows\)](#)

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

[ec2-65-0-27-66.ap-south-1.compute.amazonaws.com](#)

Username Info

[Administrator](#) ▾

Password [Get password](#)

In the Connect to Instance page , go to RDP client section and Click on Get password

Get Windows password Info

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

Instance ID

i-07708cc04eb40d2e0 (kprwindows)

Key pair associated with this instance

kprwindow

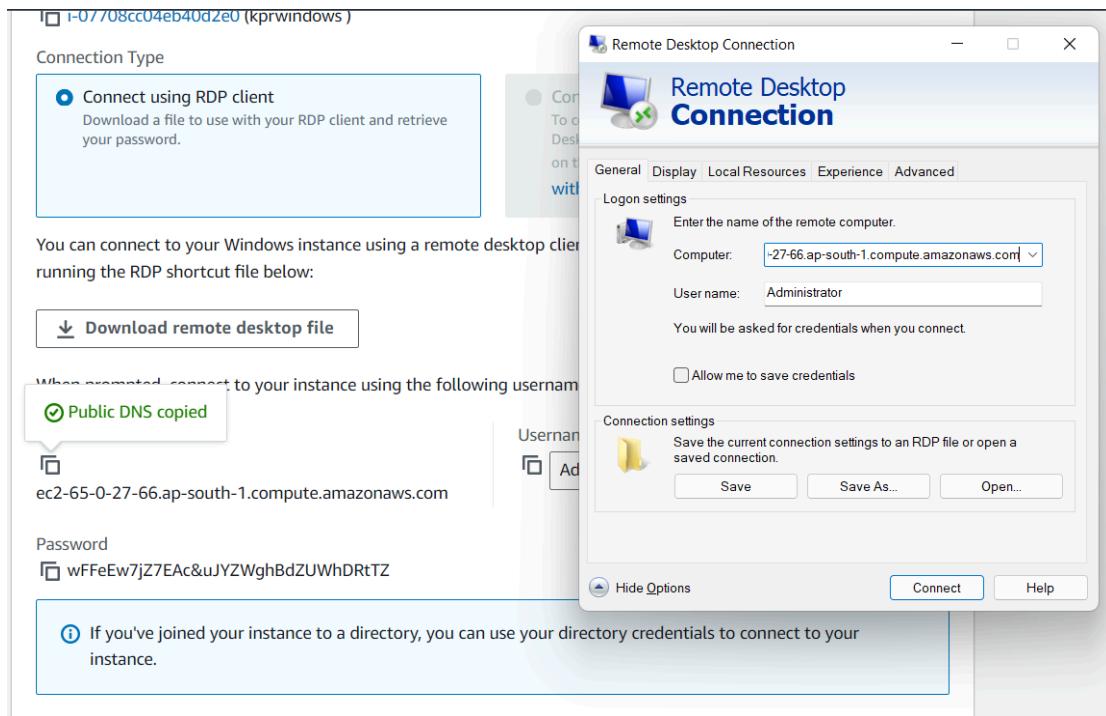
Private key

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

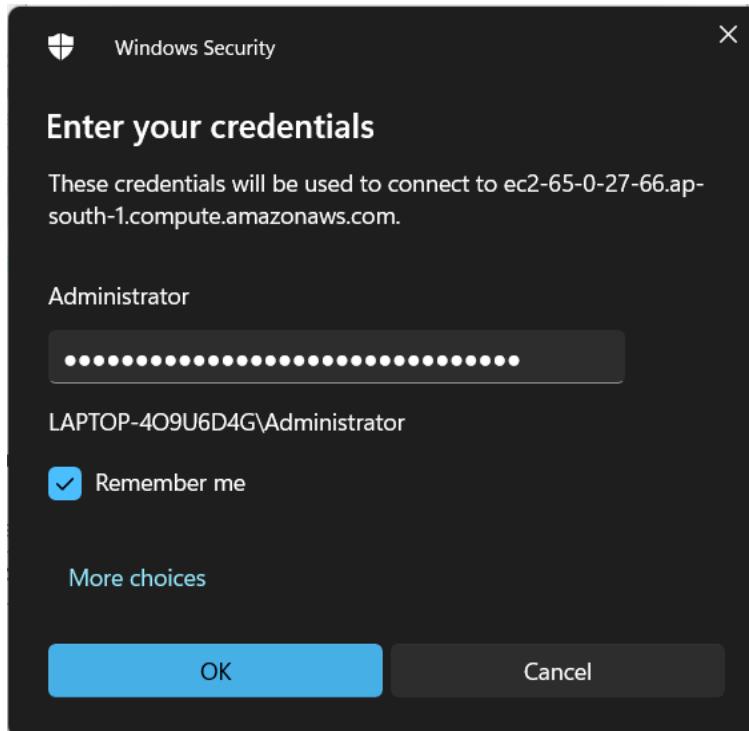
Private key contents - *optional*

```
AYl7Al/ZBY49mmt1yo+1GiBUj4Pjs4yxLj9rGc+OL3fgKj1ehrcpqeMaKOhgGTLL
aRhDejaqmhnJS2EO6cMCgYAsmn2vjTnb8ad5zGba67Yx0N1l8QRD8ZEZ9iYQjo7C
jj7vISMzfX1bLzulon9MjTHEzoOkTSPusLi4S1Go+MoME9kGGIYsSkVEZ1VobrIB
+jdQrfK25KZGRWbCx8iLPaJsLY7sPCbgAGJXELLrWEwE533/oMEuQ2LSyYGRUPw
AQKBgQDSKcZ8w9CFWluD5PB+Vto1kLnkaZT2l6BGmTJEKzSKaHAThKF9BdzMWgfU
hYh/oPyNr/mlAKG7weRK3gn2x68mNPFF7EiMVLGsgPgHLiChg6MDS2+8XaixA9rm
n2D1fD/Yd5pn0OymWB5ahp7HsBSzv/zx9xLksOSOn1q8fl5k1Q==
-----END RSA PRIVATE KEY-----
```

Copy and paste the contents of the key pair in the Private key contents box which you have created earlier and click on Decrypt password.



Once you have created the password ,open the Remote desktop Connection in your PC and enter the Public DNS in the computer section and Administrator in the username section .Click on connect



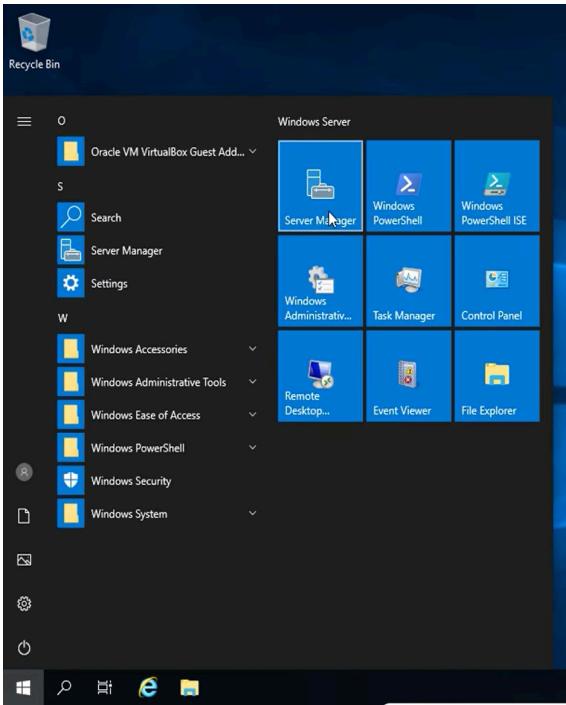
Once you click on connect , enter the password you got from the decryption of keypair



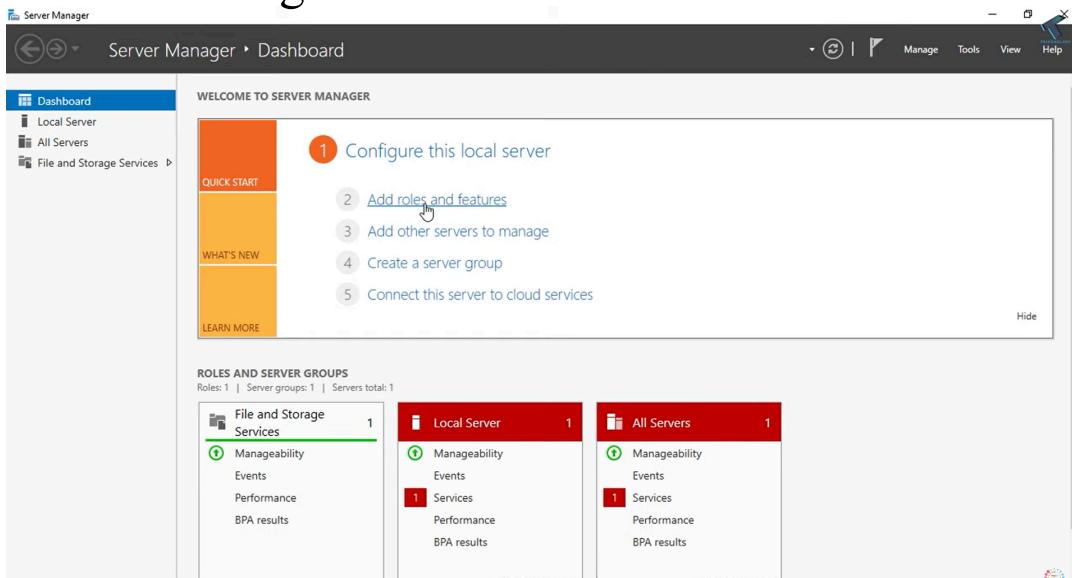
- Now create an Elastic IP address and associate it to the instance you created before.
- After associating an elastic IP, connect your instance to your windows using RDP



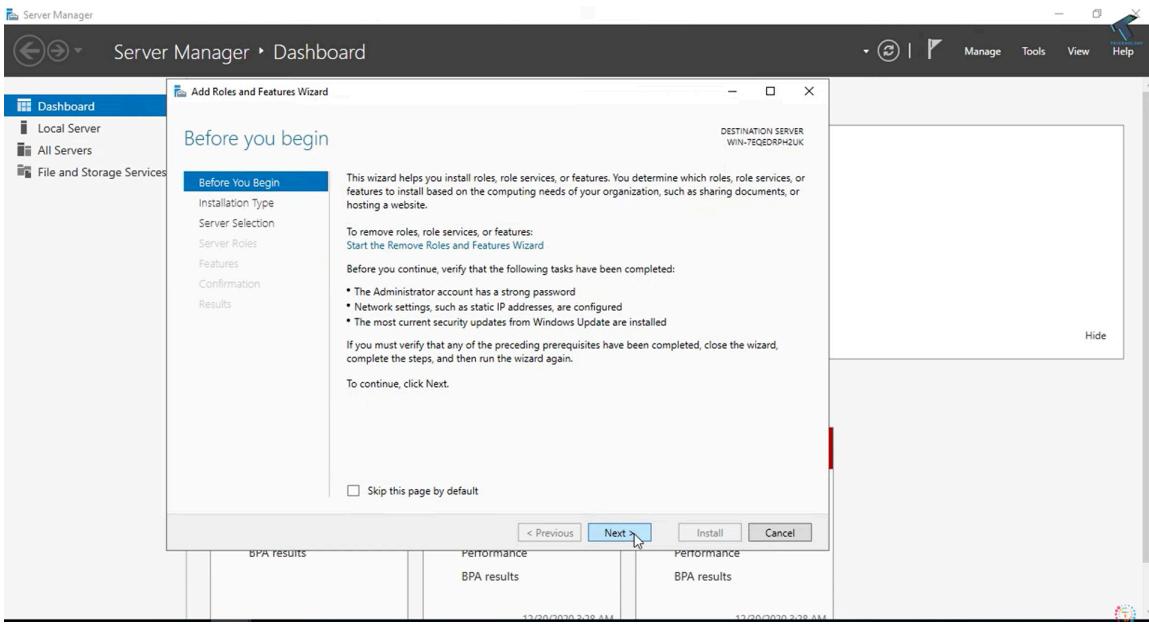
- Click on windows icon and then select server manager



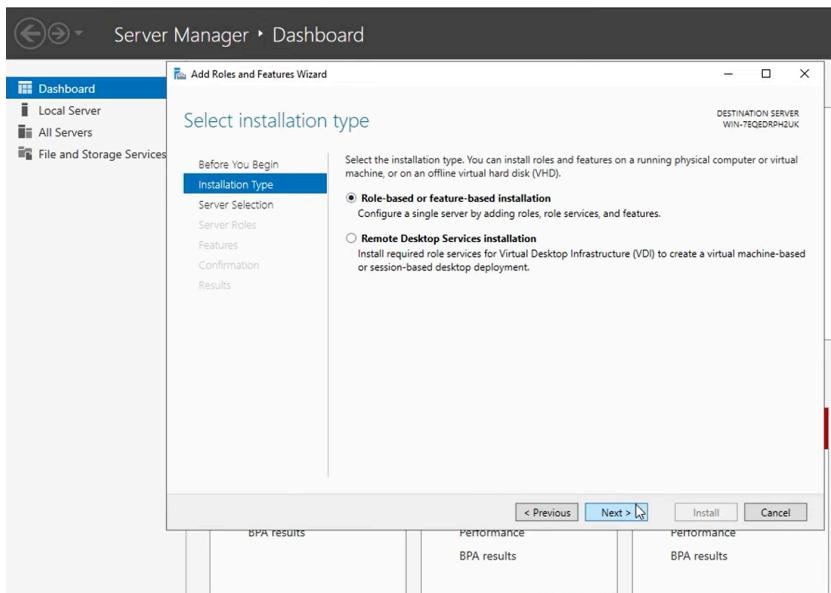
- In the server manager dashboard click on “Add roles and features”



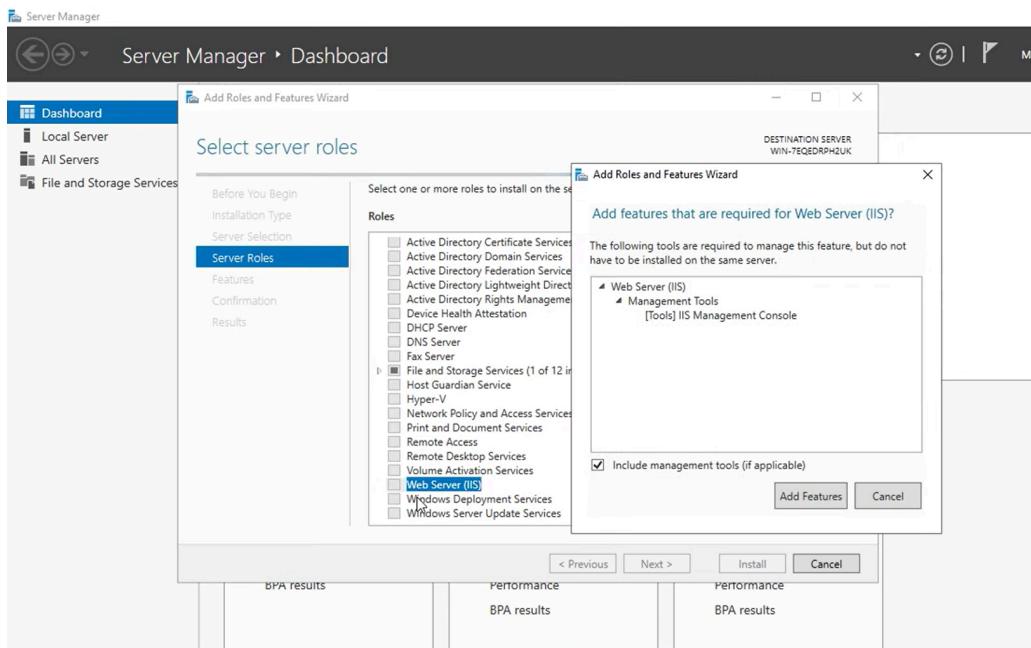
- Click on next in the upcoming popup page of ‘BEFORE YOU BEGIN’.



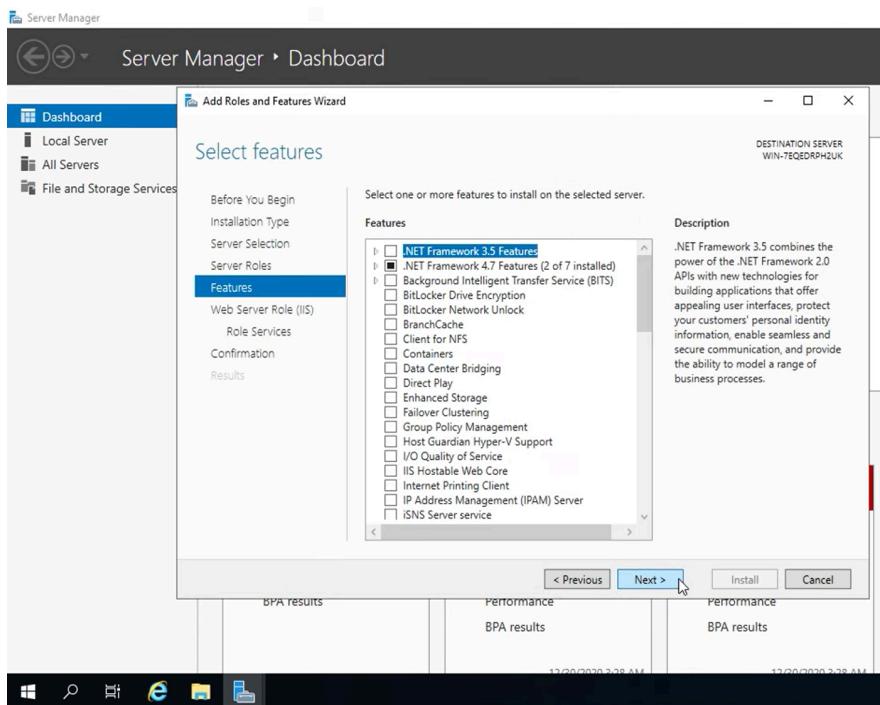
- Select Role based or feature based installation and click on next .



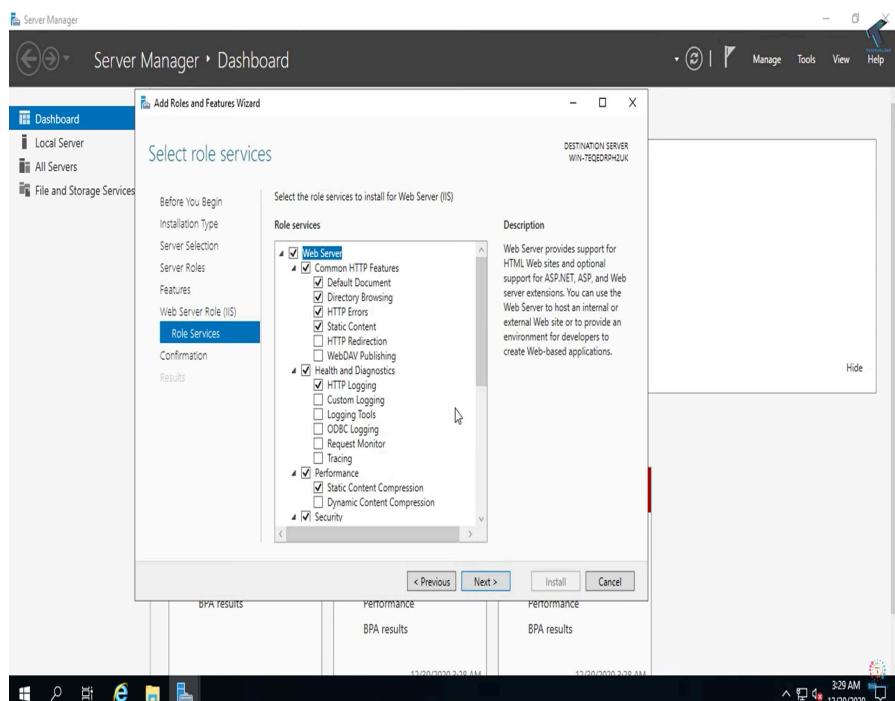
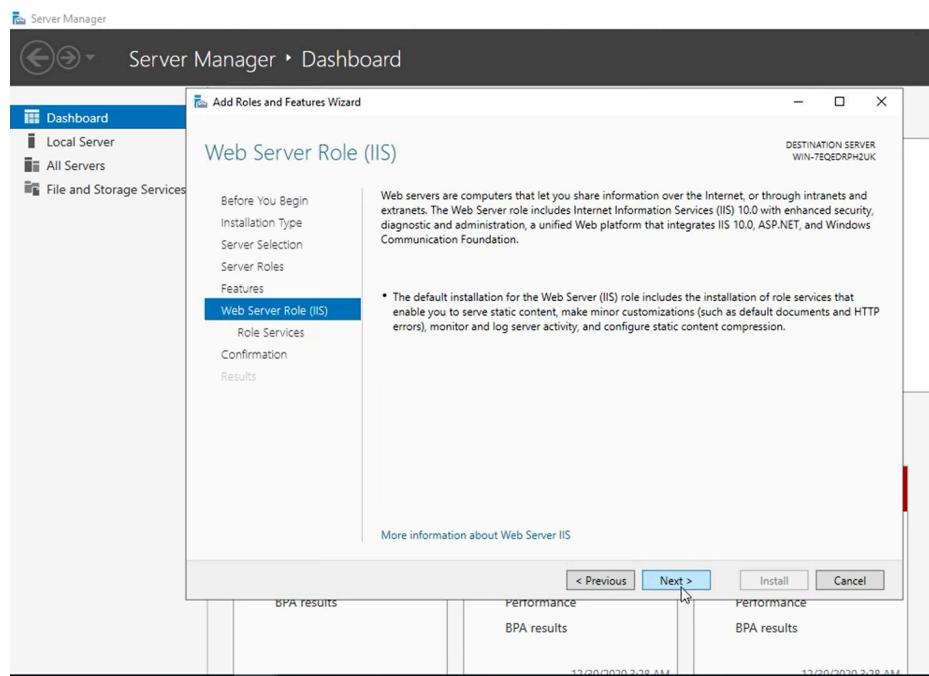
- Select web server IIS in the Roles popup and click on add features



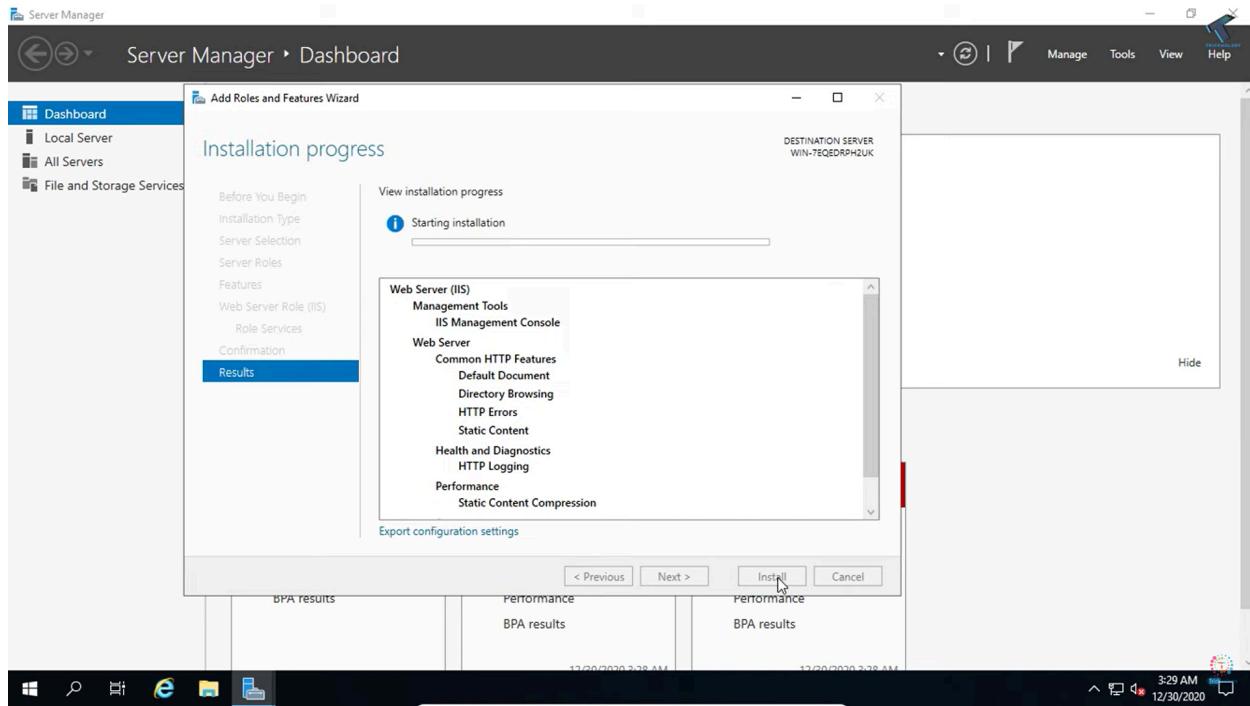
- No need to make any changes just click on next in the features page



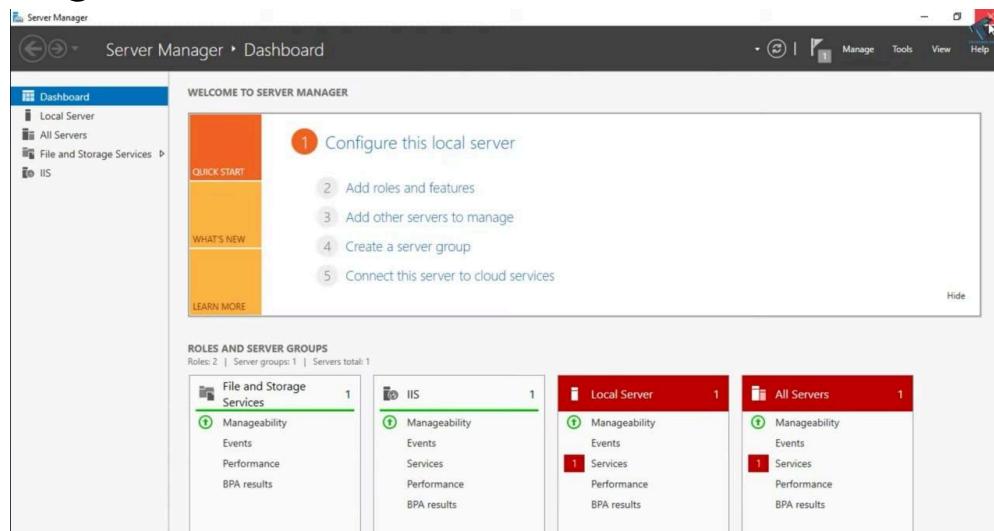
- Click on next in the web server role page



- Click on install in the installation progress page

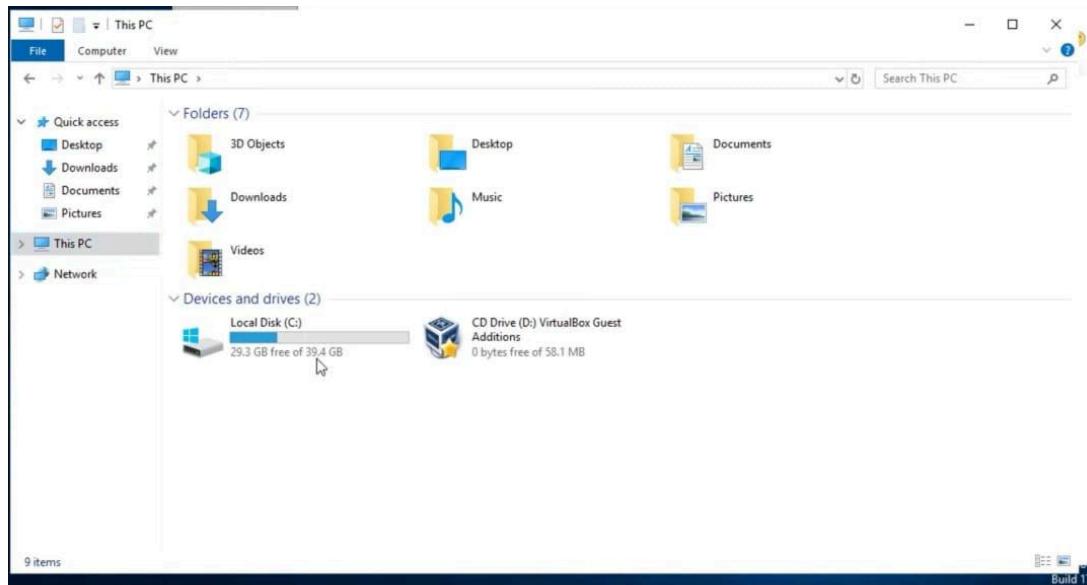


- Click on close once everything is installed .
- Once you complete all the above tasks the dashboard page will like the one below . In that you can notice the IIS has been configured.

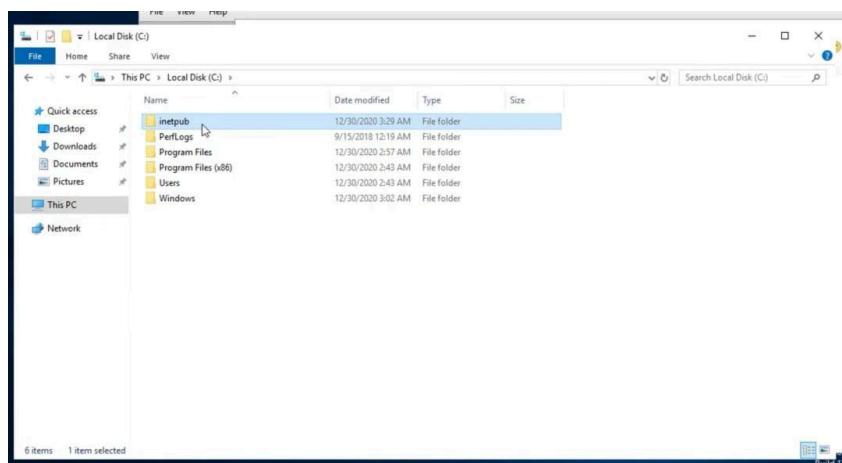


- Now if you want to add your own HTML pgm and host it. Follow these steps below .

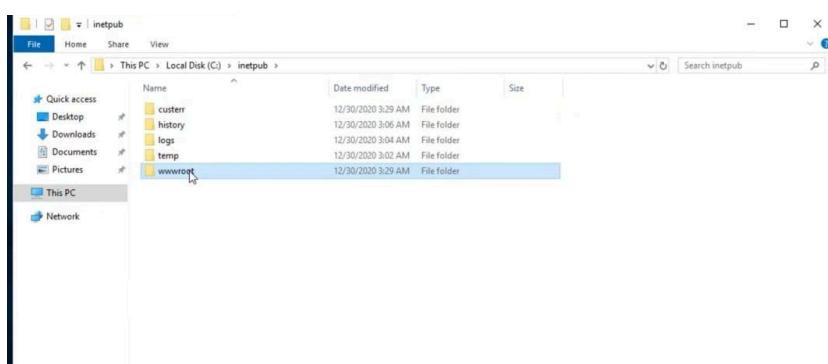
STEP1: Go to file manager and select local disk under 'This PC' option.

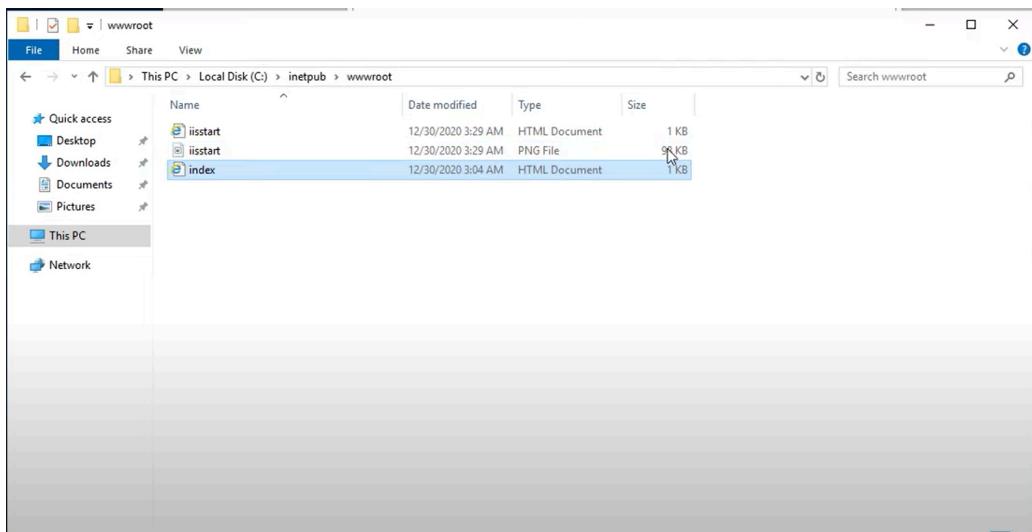


STEP 2 : In that select 'inetpub' folder .



STEP 3: Then select wwwroot folder and click on index file and edit it .





- Now you can disconnect the instance and search your public ip address of the instance in your browser and you will be connected to your webpage .

