

ASSIGNMENT-1

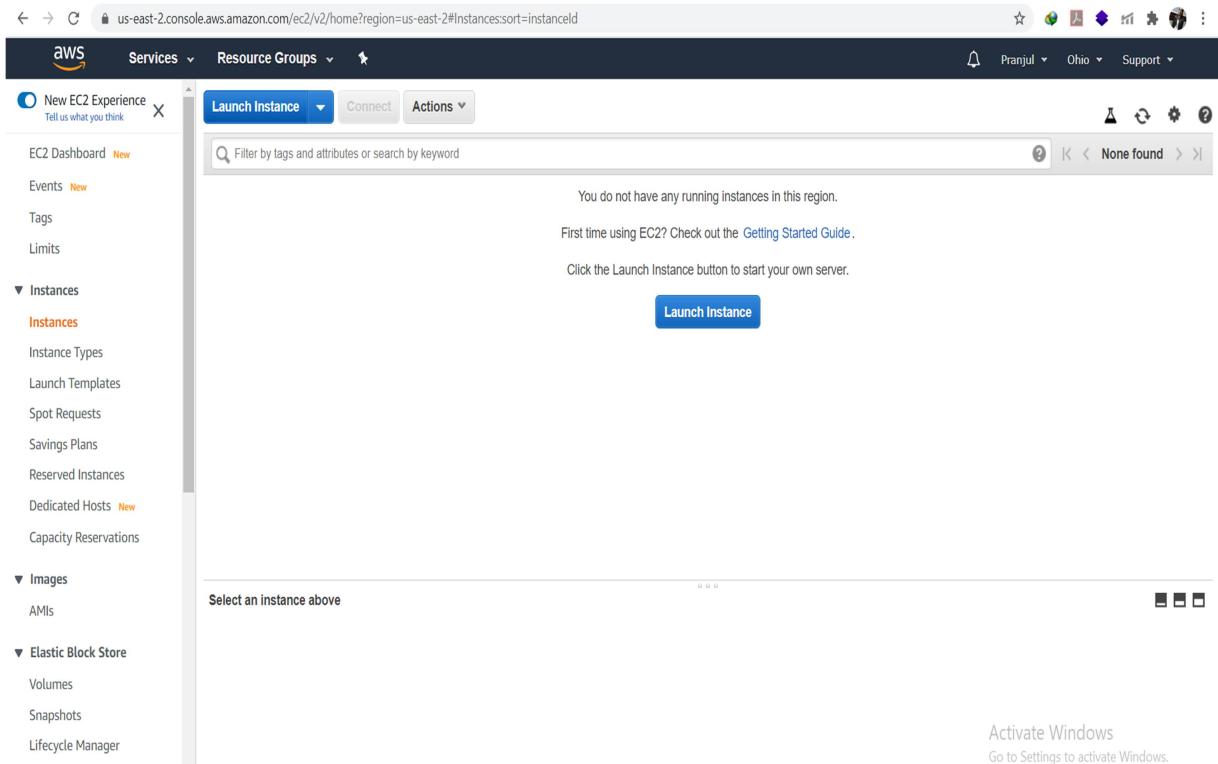
Launching one windows instance with IIS server.

- Launch one T2 micro type windows server instance on AWS.
- Configure an IIS server with default web page.

Steps:

Create an EC2 Windows Server Instance

- 1- Open the AWS EC2 Management Console.
- 2- Click on Launch Instance.



3- Choose AMI

Select Microsoft Windows Server 2019 Base (Free Tier eligible).

The screenshot shows the AWS Launch Instance Wizard Step 1: Choose an Amazon Machine Image (AMI) page. The navigation bar at the top includes links for Services, Resource Groups, and a user profile. Below the navigation is a breadcrumb trail: 1. Choose AMI (highlighted in orange), 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review.

The main content area is titled "Step 1: Choose an Amazon Machine Image (AMI)". It displays a list of available AMIs:

- SUSE Linux Enterprise Server 12 SP5 (HVM), SSD Volume Type - ami-0185282502c4b22be (Free tier eligible)
- Microsoft Windows Server 2019 Base - ami-0a83d9223efc49d6 (Free tier eligible, selected)
- Microsoft Windows Server 2019 Base with Containers - ami-0f5030e848f3f9591 (Free tier eligible)
- Microsoft Windows Server 2019 with SQL Server 2017 Standard - ami-068e444c5240485ee (Windows)

On the right side, there are "Select" buttons for each item. At the bottom, there is a section titled "Explore a serverless alternative" with a link to "Have you thought of using AWS Lambda?".

4- Choose an Instance Type i.e. t2 micro type

The screenshot shows the AWS Launch Instance Wizard Step 2: Choose an Instance Type page. The navigation bar and breadcrumb trail are identical to the previous step.

The main content area is titled "Step 2: Choose an Instance Type". It displays a table of available instance types, with the t2.micro type selected:

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	t2.micro (Free tier eligible)	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

At the bottom, there are buttons for "Cancel", "Previous", "Review and Launch", and "Next: Configure Instance Details". A note says "Go to Settings to activate Windows."

5- Configure Instance Details

The screenshot shows the AWS Launch Instance Wizard Step 3: Configure Instance Details. The page title is "Step 3: Configure Instance Details". Below it, a sub-instruction reads: "Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more." The configuration options are organized into sections:

- Number of Instances:** Set to 1.
- Purchasing option:** Request Spot instances.
- Network:** vpc-09b57162 (default). Options: Create new VPC.
- Subnet:** No preference (default subnet in any Availability Zone). Options: Create new subnet.
- Auto-assign Public IP:** Use subnet setting (Enable).
- Placement group:** Add instance to placement group.
- Capacity Reservation:** Open. Options: Create new Capacity Reservation.
- Domain join directory:** No directory. Options: Create new directory.
- IAM role:** None. Options: Create new IAM role.
- Shutdown behavior:** Stop.
- Stop - Hibernate behavior:** Enable hibernation as an additional stop behavior.
- Enable termination protection:** Protect against accidental termination.
- Monitoring:** Enable CloudWatch detailed monitoring.

At the bottom right, there are buttons for **Cancel**, **Previous**, **Review and Launch** (highlighted in blue), and **Next: Add Storage**.

6- Add Storage

The screenshot shows the AWS Launch Instance Wizard Step 4: Add Storage. The page title is "Step 4: Add Storage". Below it, a sub-instruction reads: "Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2." A table displays the current storage configuration:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MiB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0f4d67254b72fac12	30	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

A button labeled "Add New Volume" is located below the table. A note at the bottom states: "Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions." At the bottom right, there are buttons for **Cancel**, **Previous**, **Review and Launch** (highlighted in blue), and **Next: Add Tags**.

7- Add Tags

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key	(128 characters maximum)	Value	(256 characters maximum)	Instances	Volumes
This resource currently has no tags					

Choose the Add tag button or [click to add a Name tag](#).
Make sure your [IAM policy](#) includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next Configure Security Group Go to Settings to activate Windows.

8- Configure Security Groups

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Security group name:
Description:

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

⚠ Warning
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.

Cancel Previous Review and Launch Go to Settings to activate Windows.

9- Review and Launch

The screenshot shows the AWS Launch Instance Wizard at Step 7: Review Instance Launch. The top navigation bar includes links for Choose AMI, Choose Instance Type, Configure Instance, Add Storage, Add Tags, Configure Security Group, and Review. The 'Review' link is underlined, indicating the current step. Below the navigation, a section titled 'Step 7: Review Instance Launch' contains a note: 'Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.' A warning message in a yellow box states: '⚠ Improve your instances' security. Your security group, launch-wizard-1, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups'. The main content area is divided into sections: 'AMI Details' (selected), 'Instance Type', and 'Security Groups'. Under 'AMI Details', it shows Microsoft Windows Server 2019 Base - ami-0a83d9223efc49d62 (Free tier eligible). Under 'Instance Type', it lists t2.micro with 1 ECUs, 1 vCPUs, 1 GiB Memory, EBS only storage, and Low to Moderate Network Performance. Under 'Security Groups', it shows launch-wizard-1 created 2020-07-12T10:24:02Z. At the bottom right, there are 'Edit security groups', 'Activate Windows' (with a 'Cancel' button), and a large blue 'Launch' button.

10- Create an existing or create new key pair

The screenshot shows the AWS Launch Instance Wizard at Step 7: Review Instance Launch. The interface is identical to the previous screenshot, but a modal window is overlaid on the 'Security Groups' section. The modal title is 'Select an existing key pair or create a new key pair'. It contains instructions: 'A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.' A note below says: 'Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.' A dropdown menu shows 'Create a new key pair' selected. A text input field is labeled 'Key pair name' with 'joc' typed into it. A 'Download Key Pair' button is visible. A blue callout bubble provides a tip: 'You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.' At the bottom of the modal are 'Cancel' and 'Launch Instances' buttons. The background of the main page shows the same instance configuration as the previous screenshot.

← → 🔒 us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

AWS Services Resource Groups

Pranjal Ohio Support

Launch Status

Your instances are now launching
The following instance launches have been initiated: i-0f4b88d601f992b91 View launch log

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click [View Instances](#) to monitor your instances' status. Once your instances are in the **running** state, you can [connect](#) to them from the Instances screen. [Find out](#) how to connect to your instances.

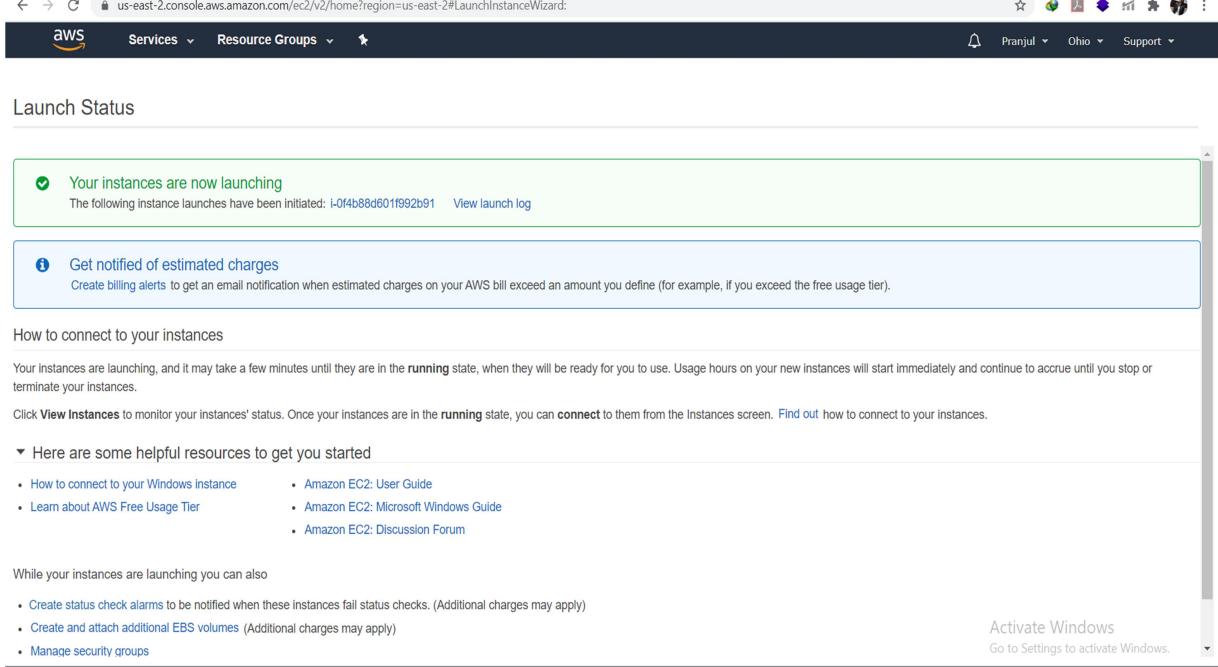
Here are some helpful resources to get you started

- How to connect to your Windows instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Microsoft Windows Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

Activate Windows
Go to Settings to activate Windows.



11- Click on view Instance.

← → 🔒 us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Instances:sort=instancetype

AWS Services Resource Groups

Pranjal Ohio Support

Instances

New EC2 Experience Tell us what you think

EC2 Dashboard New

Events New

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Launch Instance Connect Actions

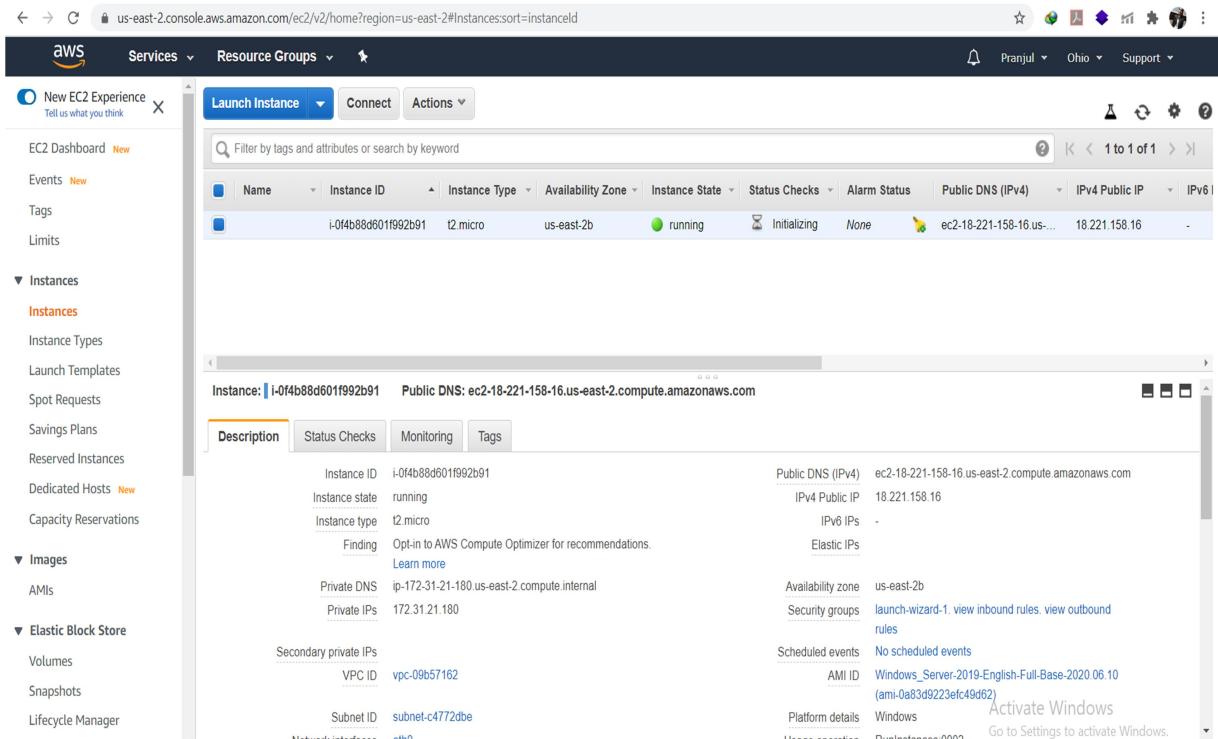
Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6
	i-0f4b88d601f992b91	t2.micro	us-east-2b	running	Initializing	None	ec2-18-221-158-16.us-east-2.compute.amazonaws.com	18.221.158.16	-

Instance: i-0f4b88d601f992b91 Public DNS: ec2-18-221-158-16.us-east-2.compute.amazonaws.com

Description Status Checks Monitoring Tags

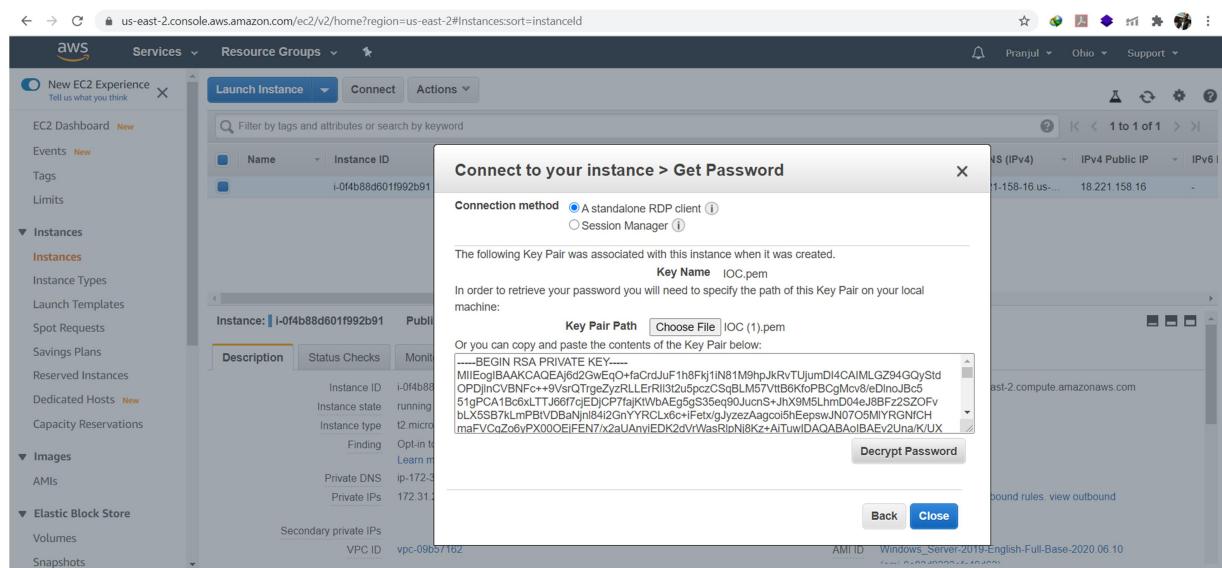
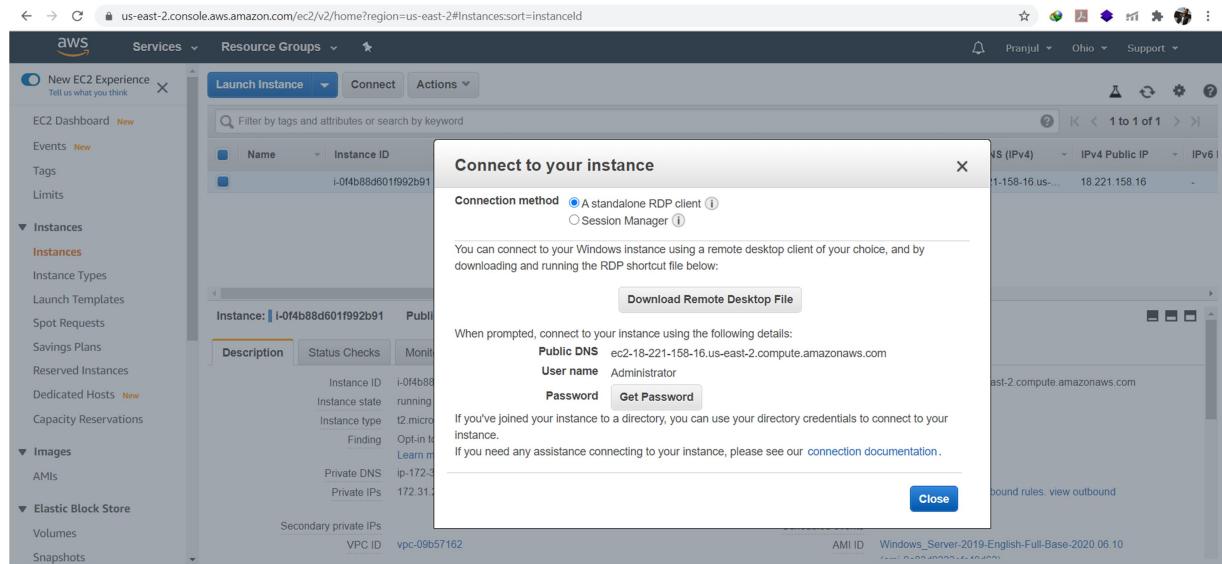
Instance ID	i-0f4b88d601f992b91	Public DNS (IPv4)	ec2-18-221-158-16.us-east-2.compute.amazonaws.com
Instance state	running	IPv4 Public IP	18.221.158.16
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations	Elastic IPs	
Learn more			
Private DNS	ip-172-31-21-180.us-east-2.compute.internal	Availability zone	us-east-2b
Private IPs	172.31.21.180	Security groups	launch-wizard-1, view inbound rules, view outbound rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-09b57162	AMI ID	Windows_Server-2019-English-Full-Base-2020.06.10 (ami-0a83d9223efc49d62)
Subnet ID	subnet-c4772dbe	Platform details	Windows
Block device mapping		Activate Windows	Go to Settings to activate Windows.

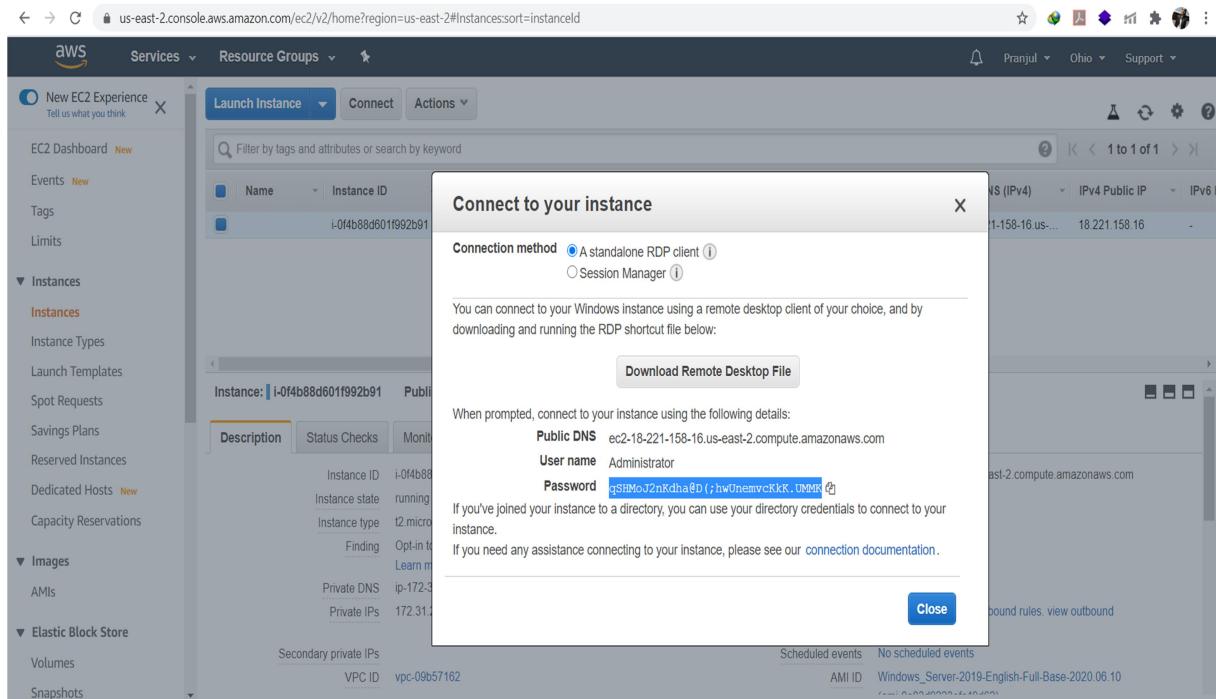


Connect

You can connect to a Windows Server machine using the Remote Desktop Connect.

- 1- In the EC2 Management Console, click Connect.
- 2- In the Connect to your instance popup, click Download Remote Desktop File.
- 3- Also click on Get Password to obtain authenticate password.
- 4- Load your private key and click Decrypt Password.

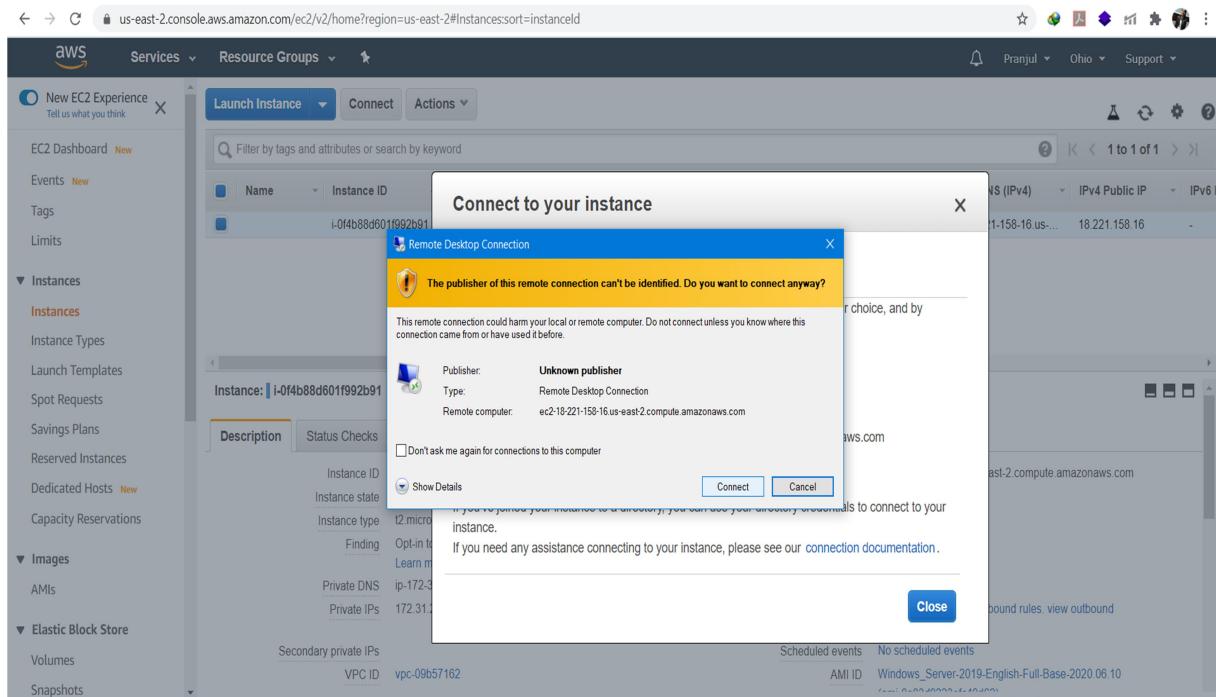




5- Open the Remote Desktop File which you have installed.

6- Click on connect.

7- Enter your credentials.



us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Instances:sort=instanceId

New EC2 Experience Tell us what you think

Services Resource Groups

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name Instance ID

i-0f4b88d601f992b91

Windows Security Enter your credentials

These credentials will be used to connect to ec2-18-221-158-16.us-east-2.compute.amazonaws.com.

Administrator [REDACTED]

DESKTOP-1FI6OP1\Administrator

Remember me

More choices

OK Cancel

Instance: i-0f4b88d601f992b91 Public DNS: ec2-18-221-158-16.us-east-2.compute.amazonaws.com

Description Status Checks Monitoring

Instance ID: i-0f4b88d601f992b91 Instance state: running Instance type: t2.micro Finding Opt-in to AMI

Private DNS: ip-172-31-21-180 us-east-2.compute.internal Private IPs: 172.31.21.180

Secondary private IPs VPC ID: vpc-09b57162 Subnet ID: subnet-c4772dbe

Availability zone: us-east-2b Security groups: launch-wizard-1, view inbound rules, view outbound rules Scheduled events: No scheduled events

AMI ID: Windows_Server-2019-English-Full-Base-2020.06.10 (ami-0a83d9223efc49d62) Platform details: Windows

Activate Windows Go to Settings to activate Windows.

us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Instances:sort=instanceId

New EC2 Experience Tell us what you think

Services Resource Groups

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name Instance ID

i-0f4b88d601f992b91

Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name: Name in the certificate from the remote computer: EC2AMAZ-A4P78NC

Certificate errors: The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

Don't ask me again for connections to this computer

View certificate... Yes No

Instance: i-0f4b88d601f992b91 Public DNS: ec2-18-221-158-16.us-east-2.compute.amazonaws.com

Description Status Checks Monitoring

Instance ID: i-0f4b88d601f992b91 Instance state: running Instance type: t2.micro Finding Opt-in to AMI

Private DNS: ip-172-31-21-180 us-east-2.compute.internal Private IPs: 172.31.21.180

Secondary private IPs VPC ID: vpc-09b57162 Subnet ID: subnet-c4772dbe

Availability zone: us-east-2b Security groups: launch-wizard-1, view inbound rules, view outbound rules Scheduled events: No scheduled events

AMI ID: Windows_Server-2019-English-Full-Base-2020.06.10 (ami-0a83d9223efc49d62) Platform details: Windows

Activate Windows Go to Settings to activate Windows.

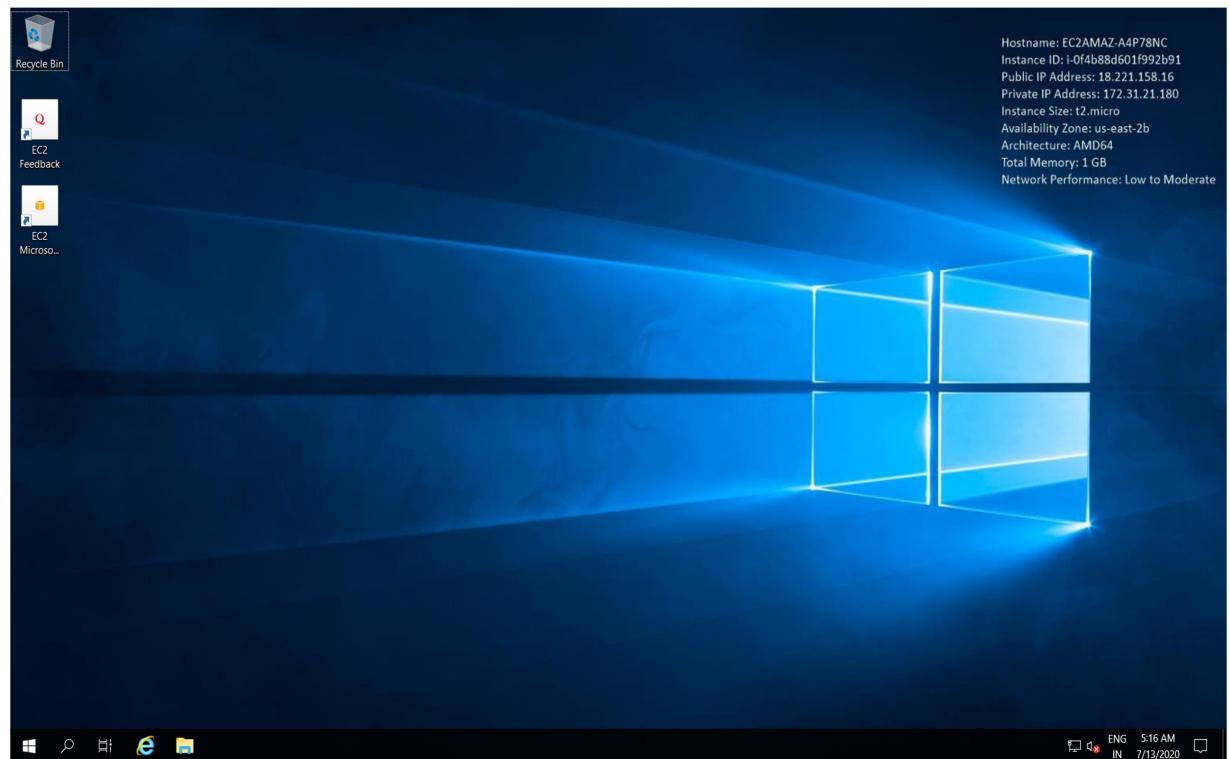
Screenshot of the AWS EC2 Instances page showing a running t2.micro instance (i-0f4b88d601f992b91). A Remote Desktop Connection window is open, connecting to the instance.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6
i-0f4b88d601f992b91	t2.micro	us-east-2b	running	2/2 checks ...	None		ec2-18-221-158-16.us...	18.221.158.16	-

Instance Details:

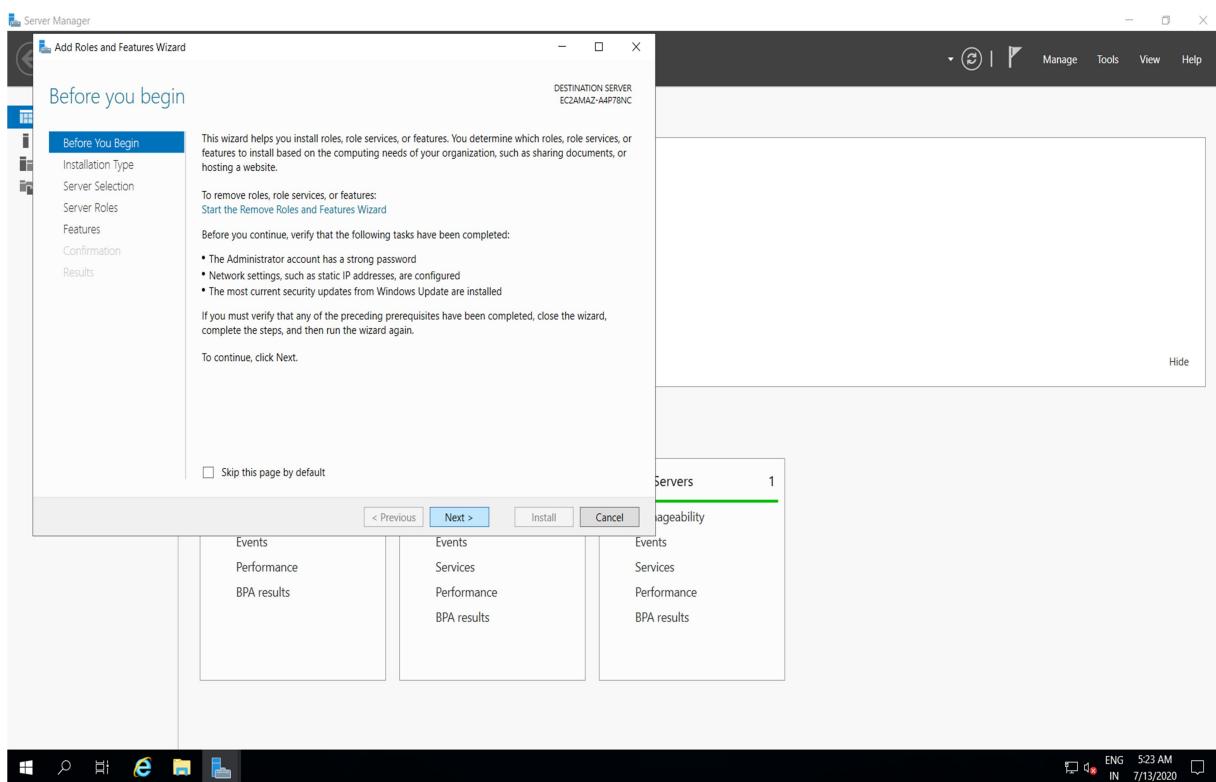
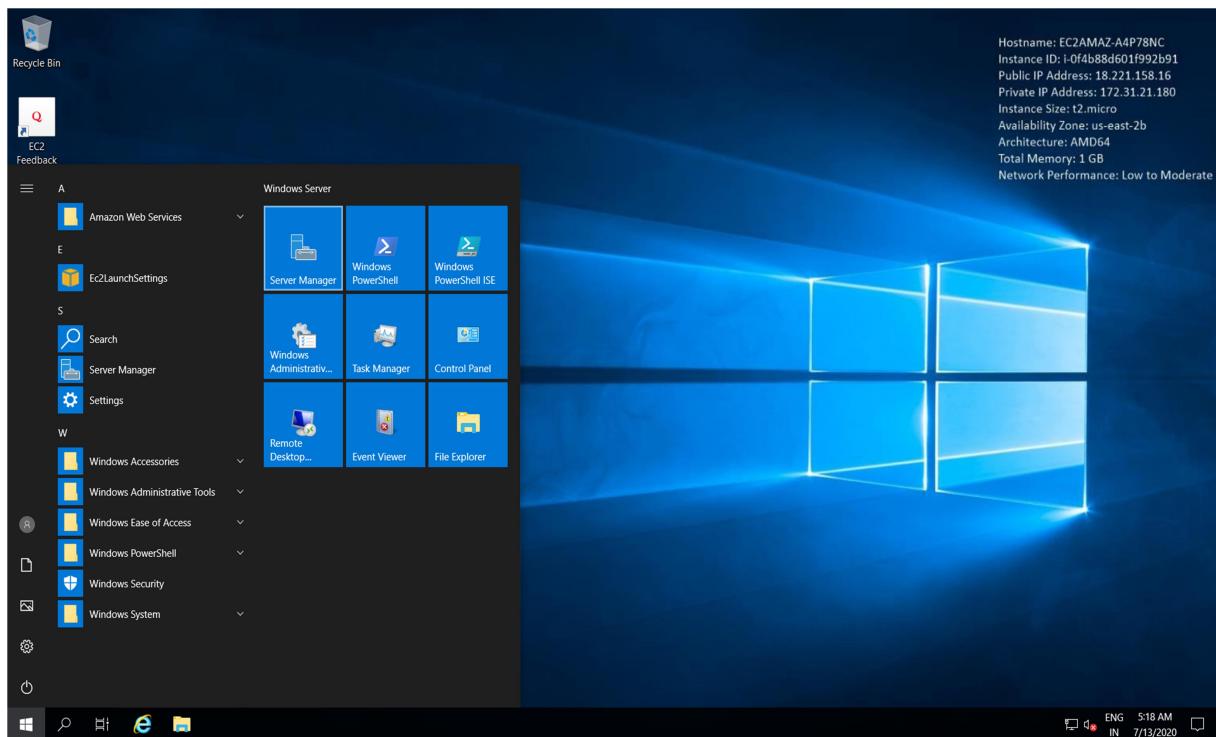
- Instance ID:** i-0f4b88d601f992b91
- Instance state:** running
- Instance type:** t2.micro
- Finding:** Opt-in to AWS Compute Optimizer for recommendations. [Learn more](#)
- Private DNS:** ip-172-31-21-180.us-east-2.compute.internal
- Private IPs:** 172.31.21.180
- Public DNS (IPv4):** ec2-18-221-158-16.us-east-2.compute.amazonaws.com
- IPv4 Public IP:** 18.221.158.16
- IPv6 IPs:** -
- Elastic IPs:** -
- Availability zone:** us-east-2b
- Security groups:** launch-wizard-1, view inbound rules, view outbound rules
- Scheduled events:** No scheduled events
- AMI ID:** Windows_Server-2019-English-Full-Base-2020.06.10 (ami-0a83d9223efc49d62)
- Platform details:** Windows
- Activate Windows:** Go to Settings to activate Windows.

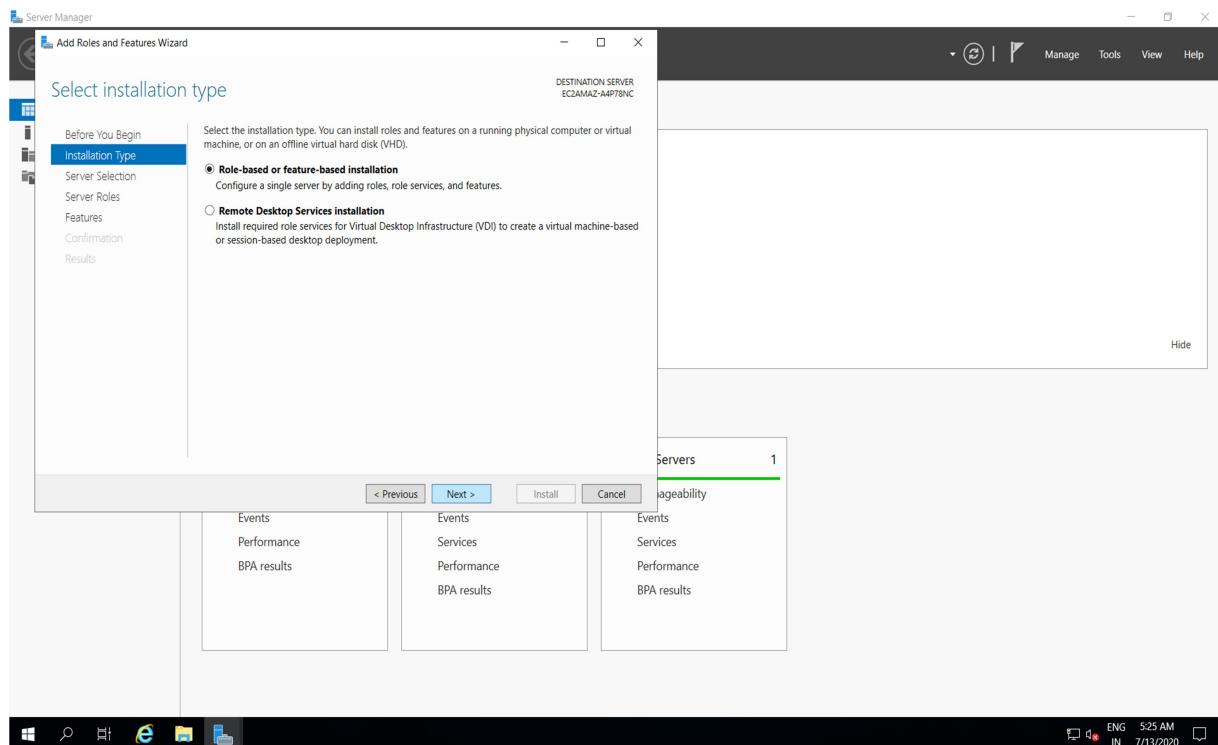
8- You are now connected to your Windows Server machine.



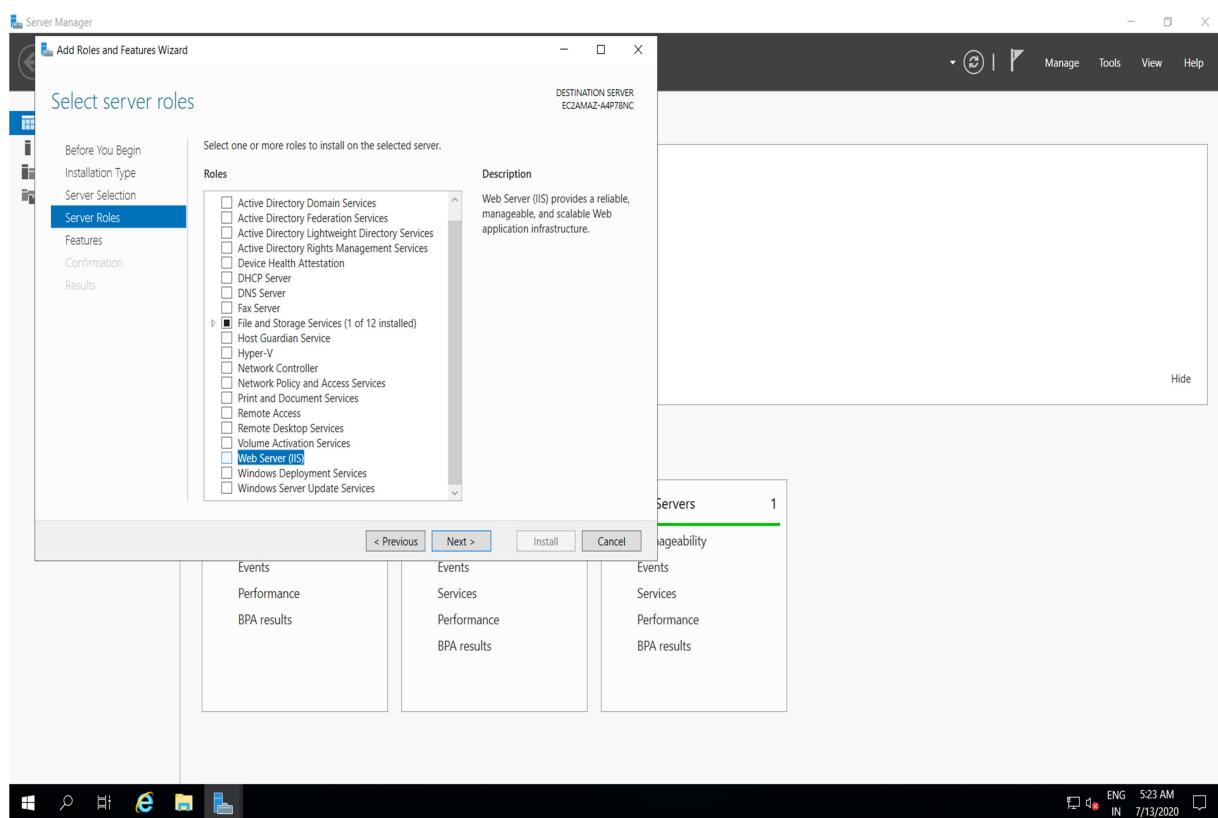
Internet Information Services (IIS)

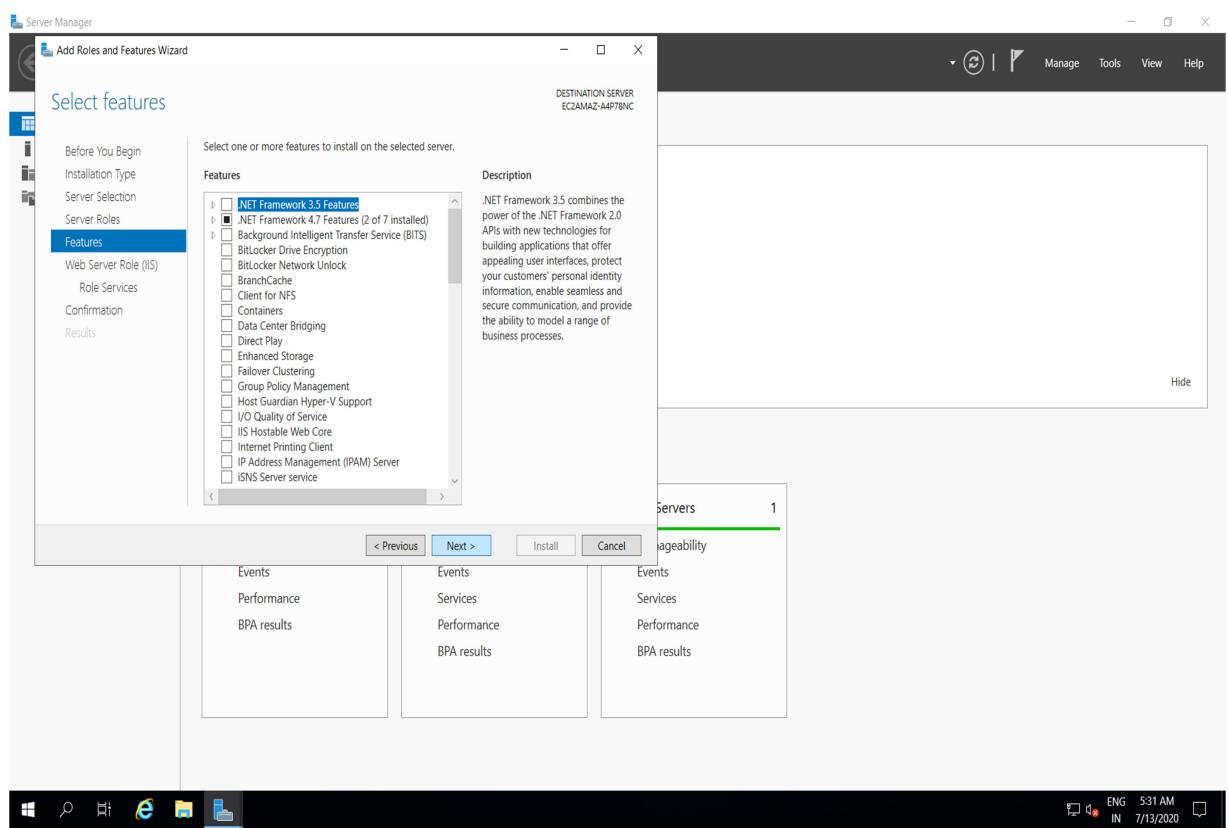
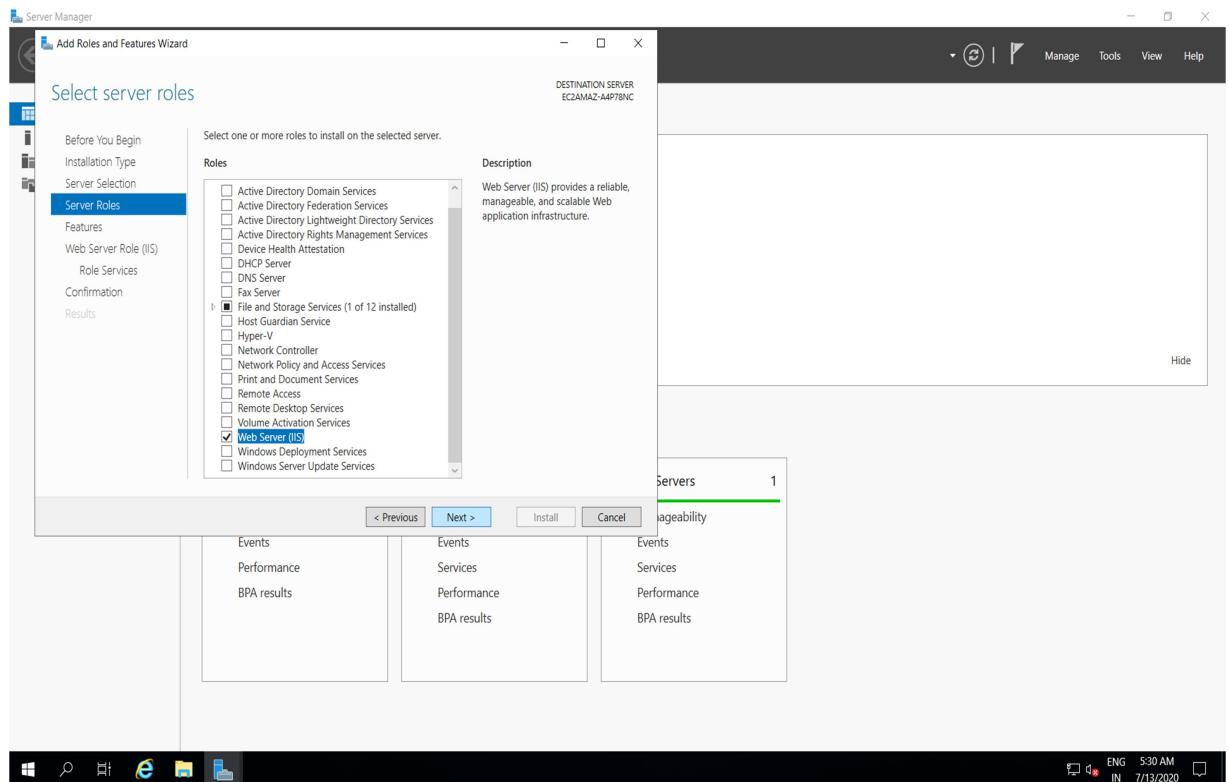
- 1- In order to enable IIS, launch Server Manager and select Manage > Add Roles and Features

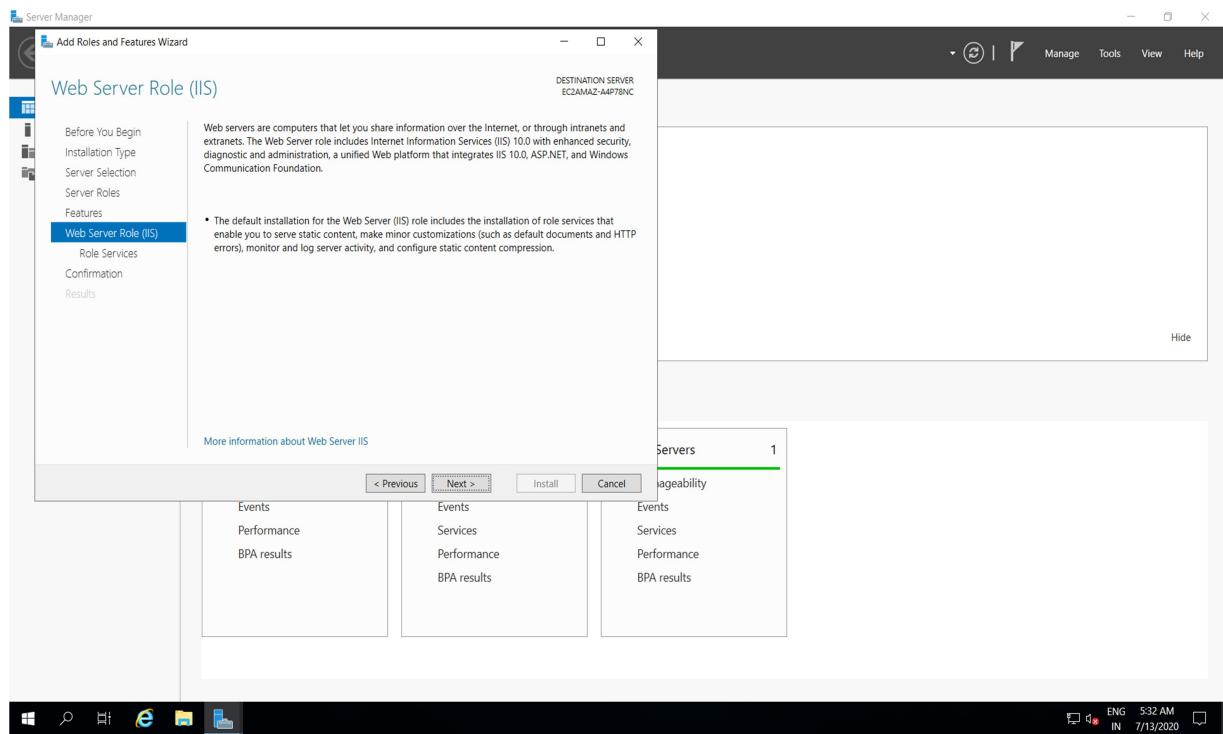




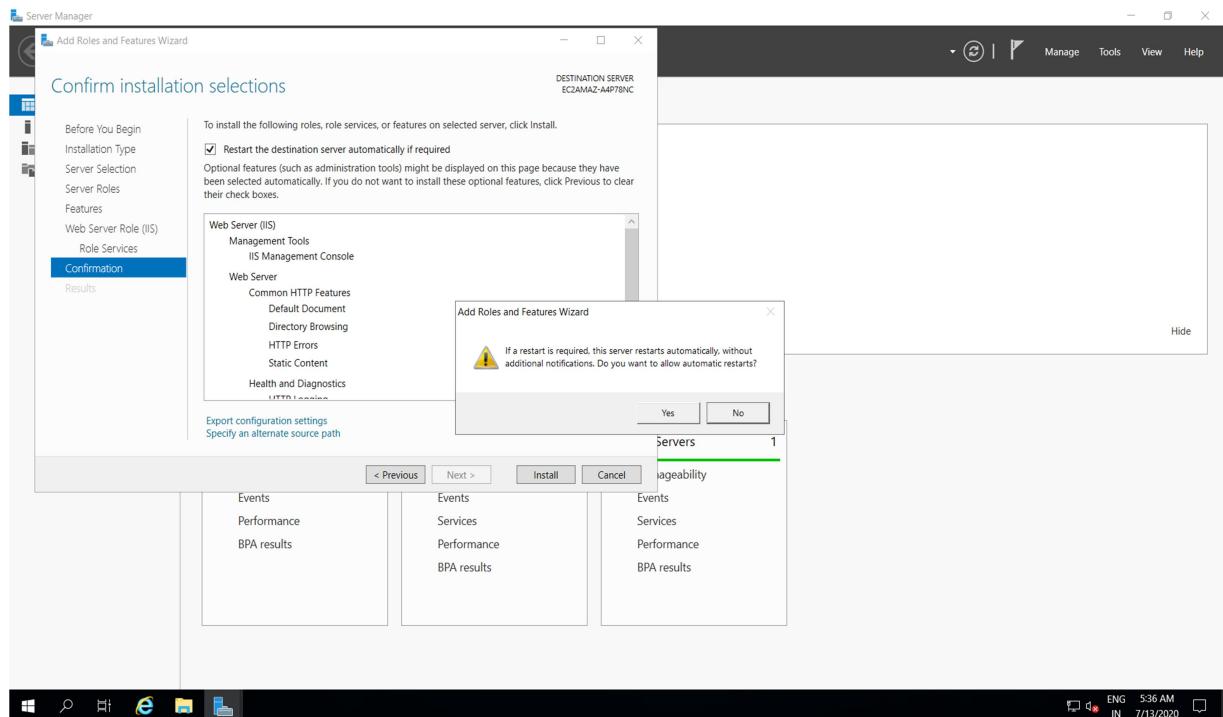
2- In Server roles choose Web Server (IIS) > Add Roles > Select Features

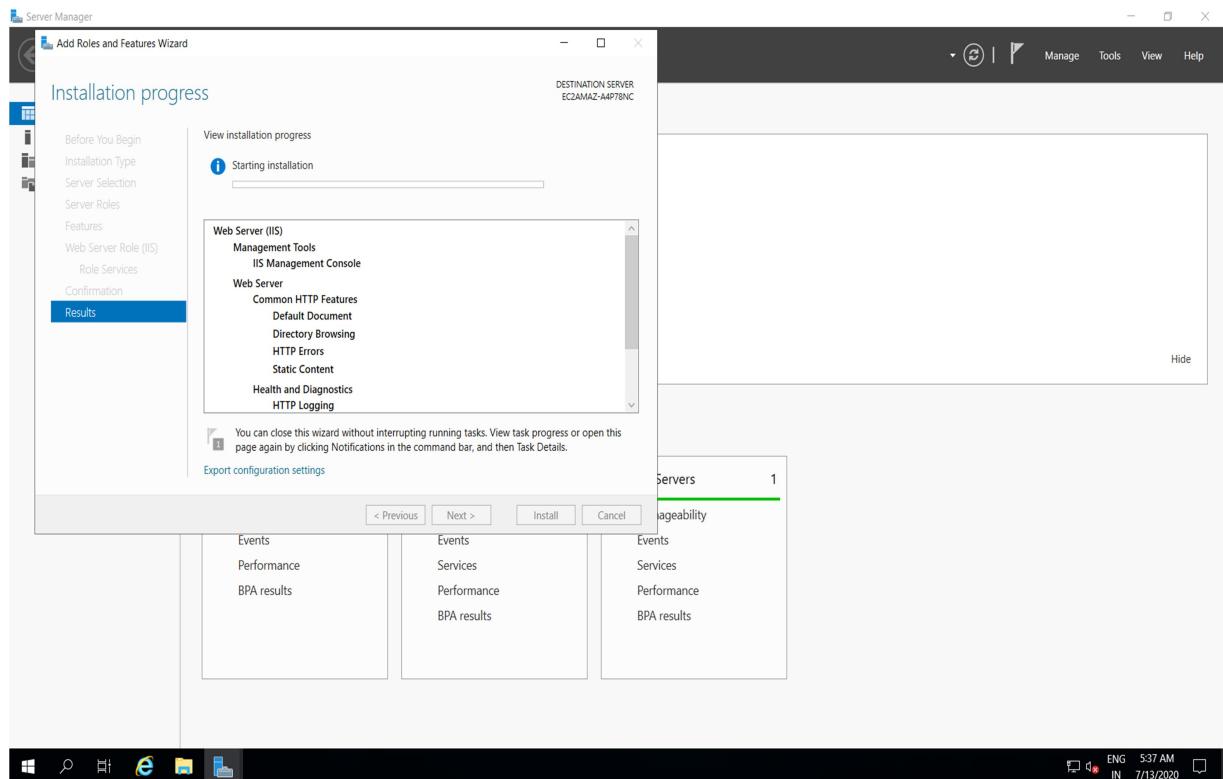




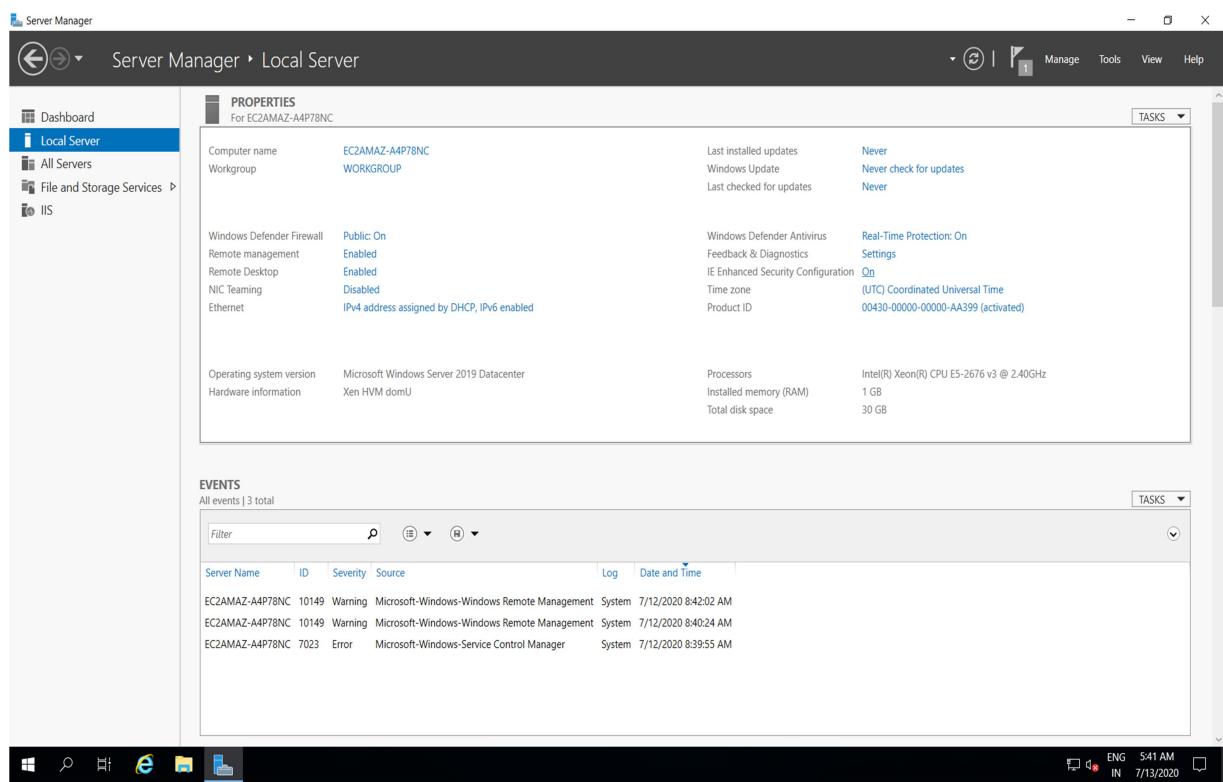


3- Click on Install, confirm installation selections





4- Now go to Local Server, click on On in Enhanced Security Configuration.



Server Manager

Server Manager • Local Server

Properties For EC2AMAZ-A4P78NC

Computer name: EC2AMAZ-A4P78NC
Workgroup: WORKGROUP

Last installed updates: Windows Update
Never
Never check for updates
Never

Windows Defender Firewall: Public On
Remote management: Enabled
Remote Desktop: Enabled
NIC Teaming: Disabled
Ethernet: IPv4 address assigned by I

Administrator: On (Recommended)
User: Off

Processor: Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz
(RAM) 1 GB
30 GB

Operating system version: Microsoft Windows Server 2019 Datacenter
Hardware information: Xen HVM domU

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.
Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrator: On (Recommended)
User: Off

More about Internet Explorer Enhanced Security Configuration

OK Cancel

Events

All events | 3 total

Filter

Server Name ID Severity Source

EC2AMAZ-A4P78NC 10149 Warning Microsoft-Windows-Windows Remote Management System 7/12/2020 8:42:02 AM
EC2AMAZ-A4P78NC 10149 Warning Microsoft-Windows-Windows Remote Management System 7/12/2020 8:40:24 AM
EC2AMAZ-A4P78NC 7023 Error Microsoft-Windows-Service Control Manager System 7/12/2020 8:39:55 AM

TASKS

ENG 5:41 AM IN 7/13/2020

The screenshot shows the Windows Server Manager interface. The left sidebar has 'Local Server' selected. The main pane shows 'PROPERTIES For EC2AMAZ-A4P78NC'. It includes sections for Computer name, Workgroup, Windows Defender Firewall, Remote management, NIC Teaming, Ethernet, Operating system version, and Hardware information. A modal dialog titled 'Internet Explorer Enhanced Security Configuration' is open, showing settings for Administrators and Users. Below the properties are 'EVENTS' and a list of three system events. The taskbar at the bottom shows standard icons and the date/time: 'ENG 5:41 AM IN 7/13/2020'.

5- Open File Explorer > Local Disk(C) > inetpub > wwwroot

Recycle Bin

Feedback

EC2 Microso...

This PC

File Computer View

Folders (7)

- 3D Objects
- Desktop
- Downloads
- Music
- Pictures
- Videos

Devices and drives (1)

- Local Disk (C): 16.4 GB free of 29.9 GB, Space free: 16.4 GB, Total size: 29.9 GB

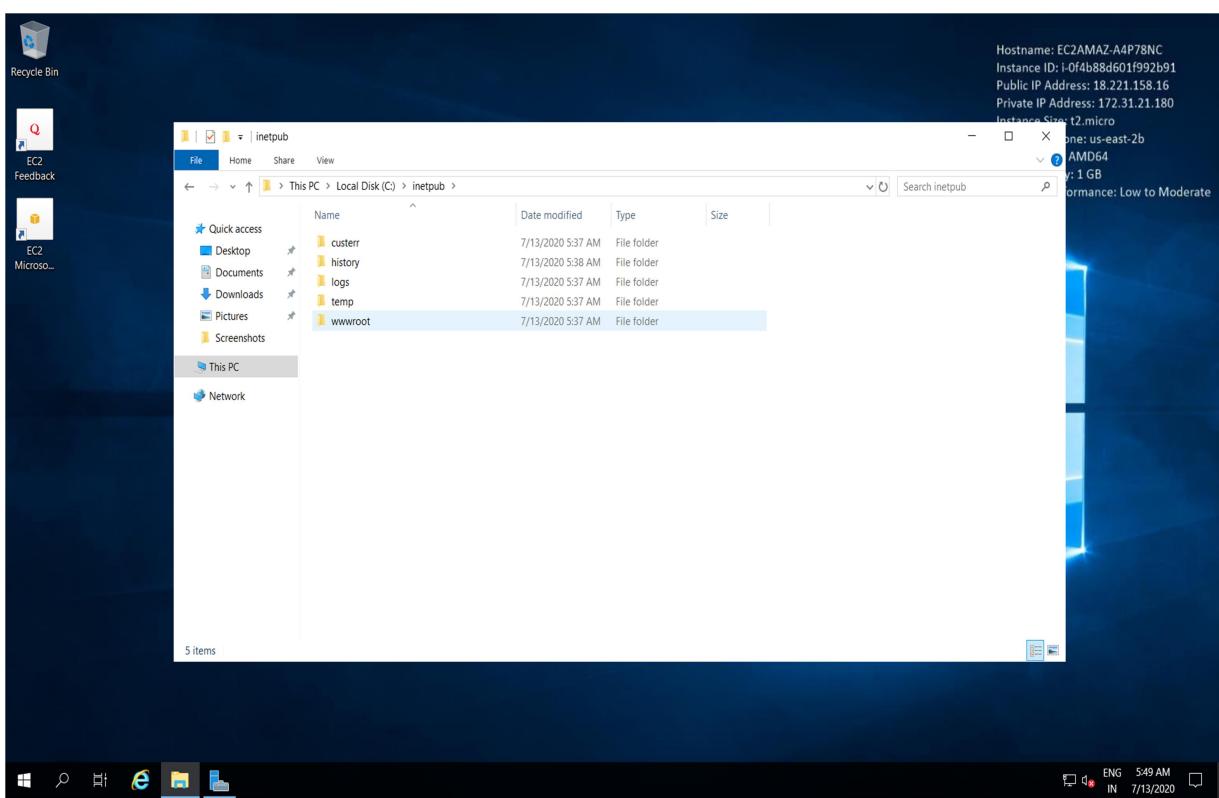
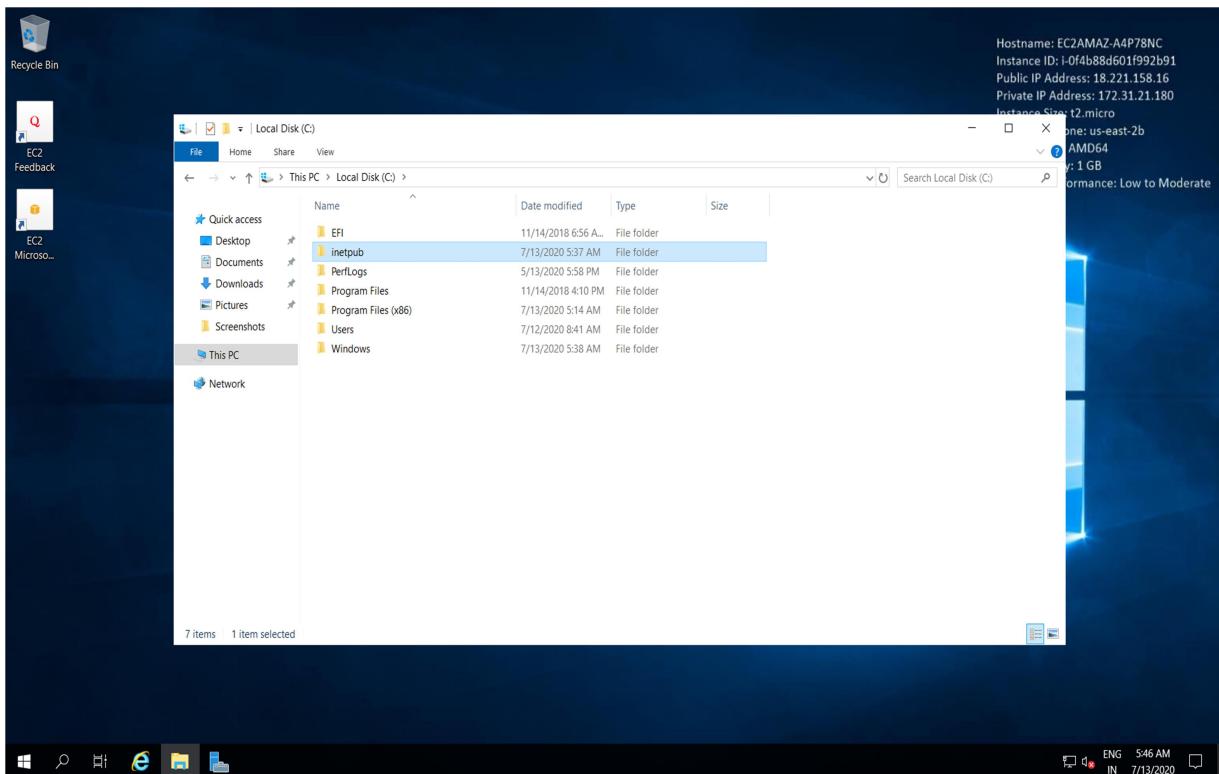
Hostname: EC2AMAZ-A4P78NC
Instance ID: i-0f4b88d601f992b91
Public IP Address: 18.221.158.16
Private IP Address: 172.31.21.180
Instance Status: t2.micro
Volume: us-east-2b
Type: AMD64
Memory: 1 GB
Performance: Low to Moderate

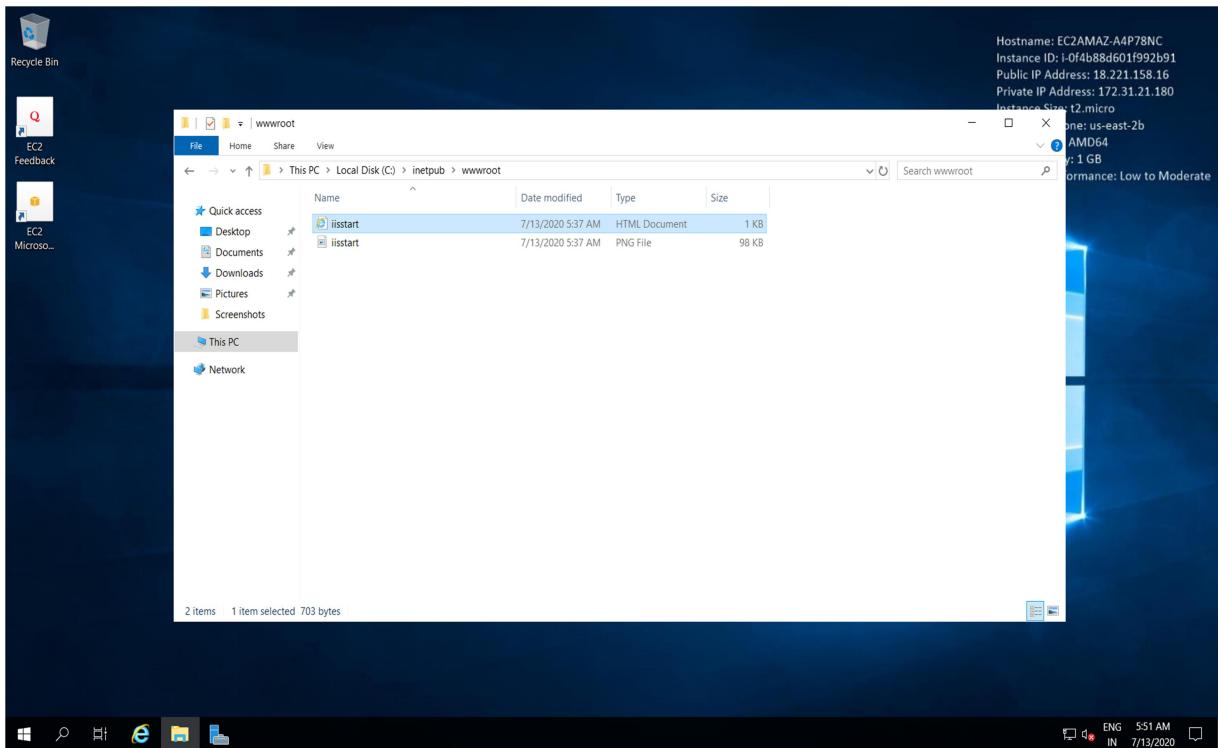
Search This PC

8 items

ENG 5:45 AM IN 7/13/2020

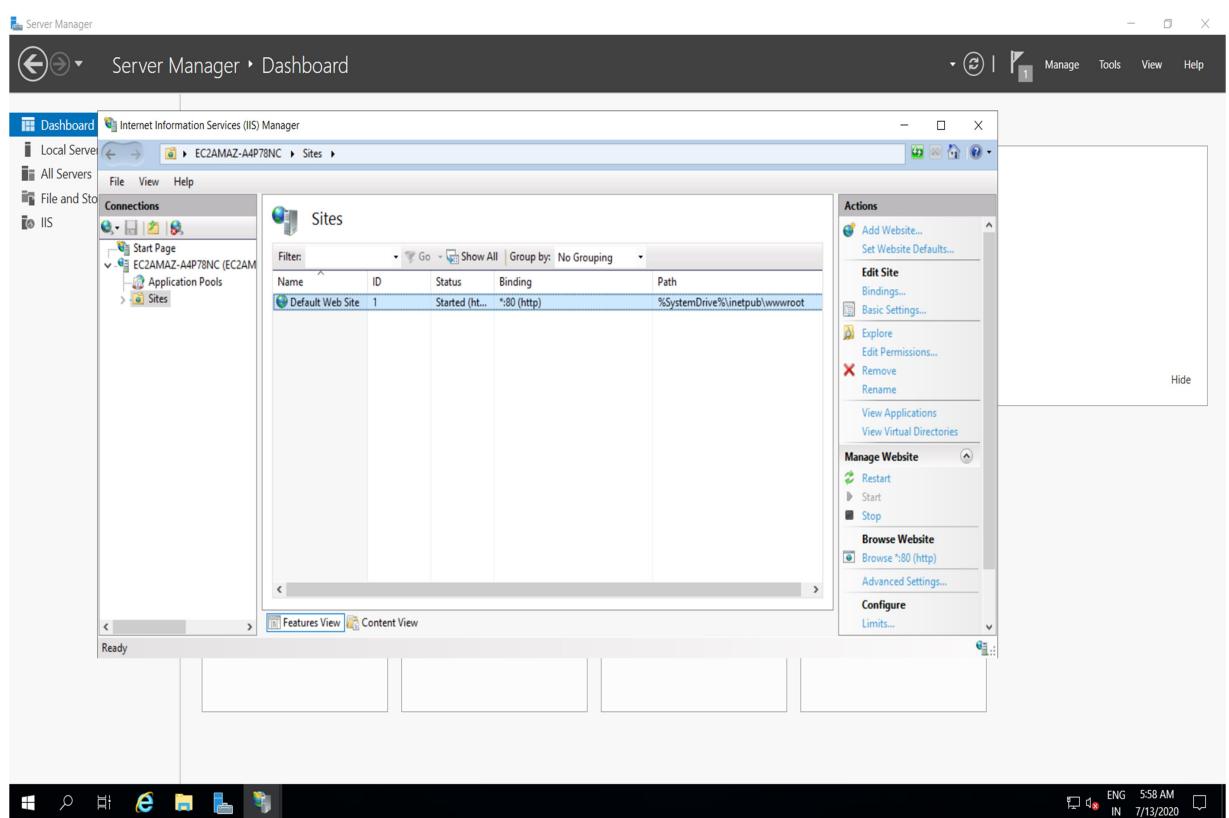
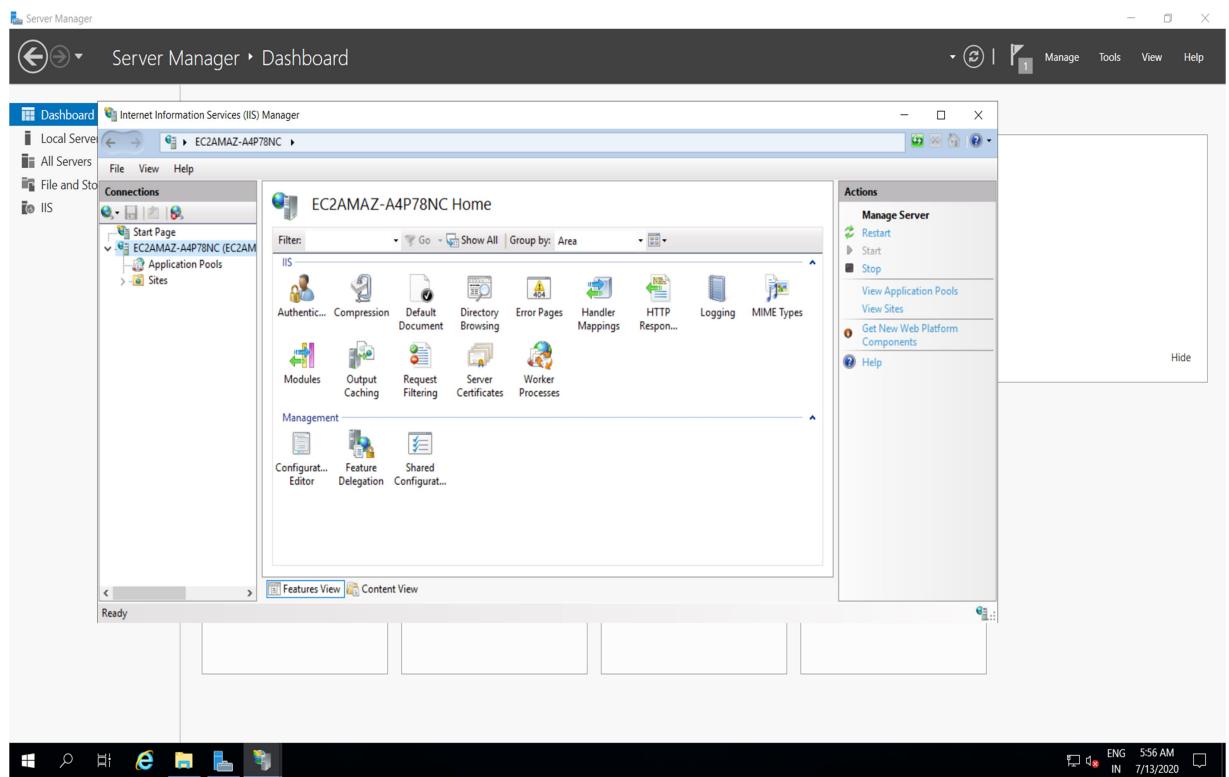
The screenshot shows the Windows File Explorer interface. The left sidebar lists 'This PC' and 'Network'. The main pane shows 'Folders (7)' and 'Devices and drives (1)'. Under 'Devices and drives (1)', 'Local Disk (C)' is selected, showing its free space (16.4 GB), total size (29.9 GB), and usage details. A status bar at the top right provides instance details: Hostname: EC2AMAZ-A4P78NC, Instance ID: i-0f4b88d601f992b91, Public IP Address: 18.221.158.16, Private IP Address: 172.31.21.180, Instance Status: t2.micro, Volume: us-east-2b, Type: AMD64, Memory: 1 GB, and Performance: Low to Moderate. The taskbar at the bottom shows standard icons and the date/time: 'ENG 5:45 AM IN 7/13/2020'.





6- Again go to Dashboard > Tools > IIS Manager

A screenshot of the Microsoft Server Manager dashboard. On the left, there's a navigation menu with 'Dashboard' selected, followed by 'Local Server', 'All Servers', 'File and Storage Services', and 'IIS'. The main area is titled 'WELCOME TO SERVER MANAGER' and features a 'QUICK START' section with five numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this is a 'ROLES AND SERVER GROUPS' section showing four categories: 'File and Storage Services' (1 item), 'IIS' (1 item), 'Local Server' (1 item), and 'All Servers' (1 item). Each category has a list of management tools: 'Manageability', 'Events', 'Performance', and 'BPA results'. On the right side, a vertical navigation bar lists various management tools, with 'Internet Information Services (IIS) Manager' currently highlighted. The taskbar at the bottom is identical to the one in the previous screenshot.



7- Click on Default Web Site 1

8- From right hand side Browse Website.

