

Advance AWS

AWS Project- 1

Student:

Kishore Shinde

Teacher:

Mrs. Vinolin Jeremiah

Course:

Advance AWS Cloud Computing with DevOps
Fundamentals

Institute:

Lets Upgrade

Project 01:

Deploying a Web Server (IIS) in Windows Instance

Below are the 4 steps:

STEP A: Launch an Amazon EC2 Windows Instance

STEP B: Connect EC2 Instance

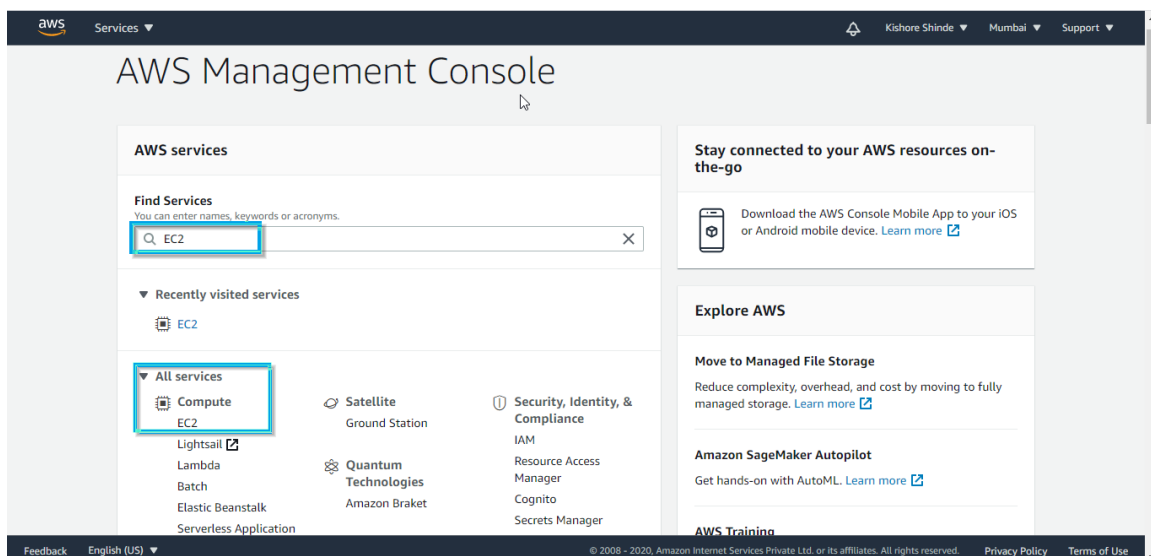
STEP C: Install IIS Server

STEP D: Terminate EC2 Instance

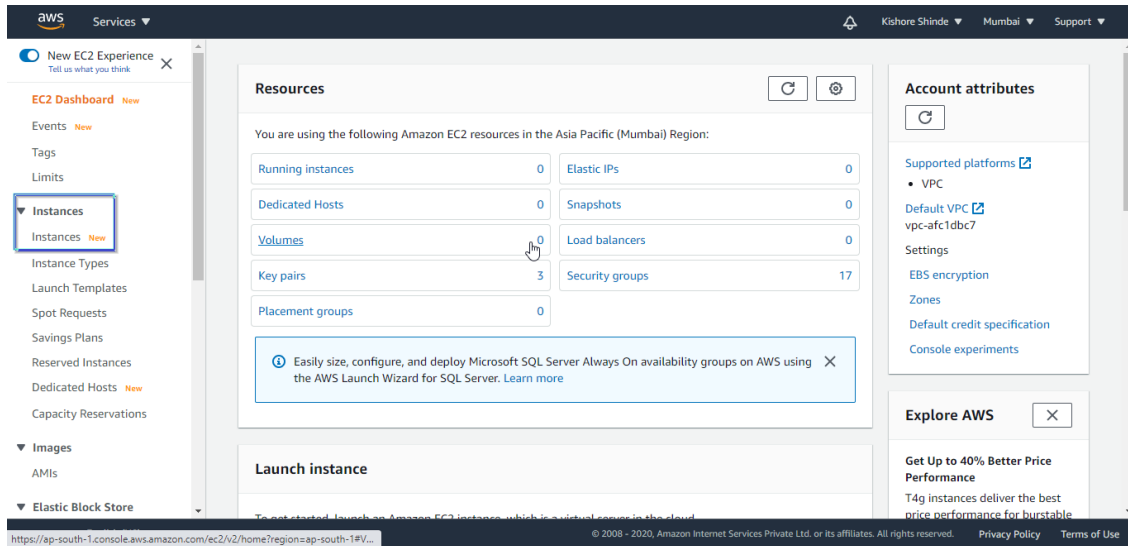
STEP A: Launch an Amazon EC2 Instance

Steps for launching a new windows instance:

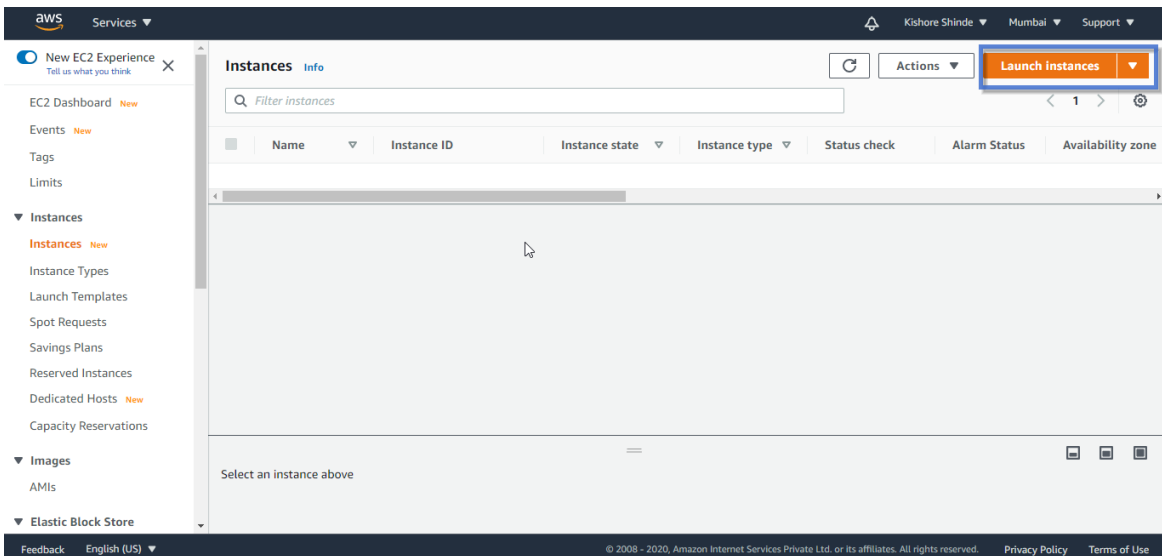
1. From the AWS Management Console, you can either find EC2 service or click on All services ->Compute->EC2



2. Once you are in EC2 console from the EC2 Dashboard on the left, select Instances

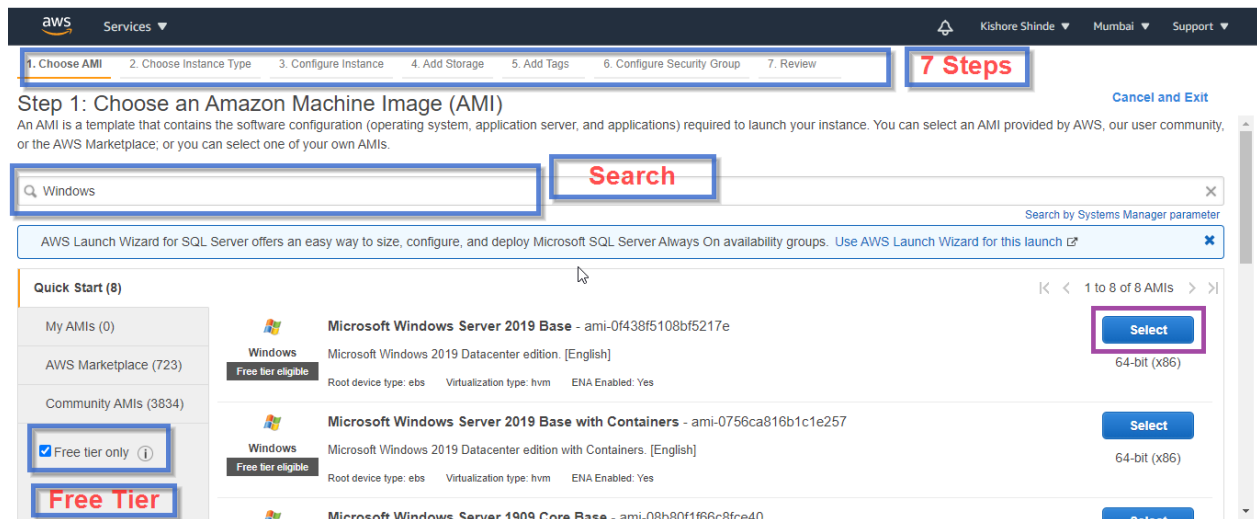


3. From the Instances Dashboard, Select Launch Instance at the right



Once you click on Launch Instance, a wizard will start which has 7 steps for creating the instance.

Step 1: Choose an Amazon Machine Image (AMI)



You can search the AMI e.g. Windows.... or can select the AMI from the list of the AMI's.

Note: Make sure you select the Free Tier only option so only free AMI's will be shown and you will not be charged.

Click on "Select" on the Windows AMI e.g. Microsoft Windows 2019 Base.

Step 2: Choose an Instance Type

Here you can select the Instance type. These are varying combinations of CPU, Memory, Storage and Networking capacity. The default instance type selected is "t2.micro" which is Free tier eligible. Let it be selected otherwise you will be charged for other instance type. You can even see the details of the selected instance type in **Currently Selected**

e.g. : t2.micro (Variable ECUs,1 vCPUs,2.5 GHz,Intel Xeon Family, 1 GiB memory, EBS only)

aws Services

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Step 3 : Configure Instance Details

Here you can configure the instance that suits your requirement. You can launch multiple instances from the same AMI you can mention it in Number of instances.

In Network you can select the VPC or create new VPC, we will continue with default VPC, select or create new Subnet, we will continue with default subnet. We can select IAM role, we will continue with "None".

aws Services

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

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.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: ☐ Request Spot instances

Network: vpc-afc1dbc7 (default) Create new VPC

Subnet: No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: ☐ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory Create new directory

IAM role: None Create new IAM role

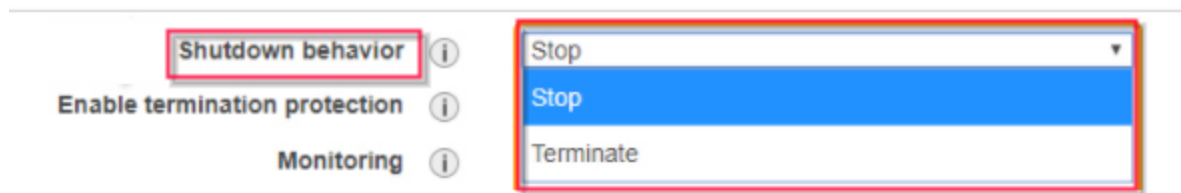
Shutdown behavior: Stop

Stop - Hibernate behavior: ☐ Enable hibernation as an additional stop behavior

Enable termination protection: ☐ Protect against accidental termination

Cancel Previous Review and Launch Next: Add Storage

In the Shutdown behavior you can select Stop or Terminate. It is an important option If you select Stop when the instance shuts down it will not be deleted but stopped.



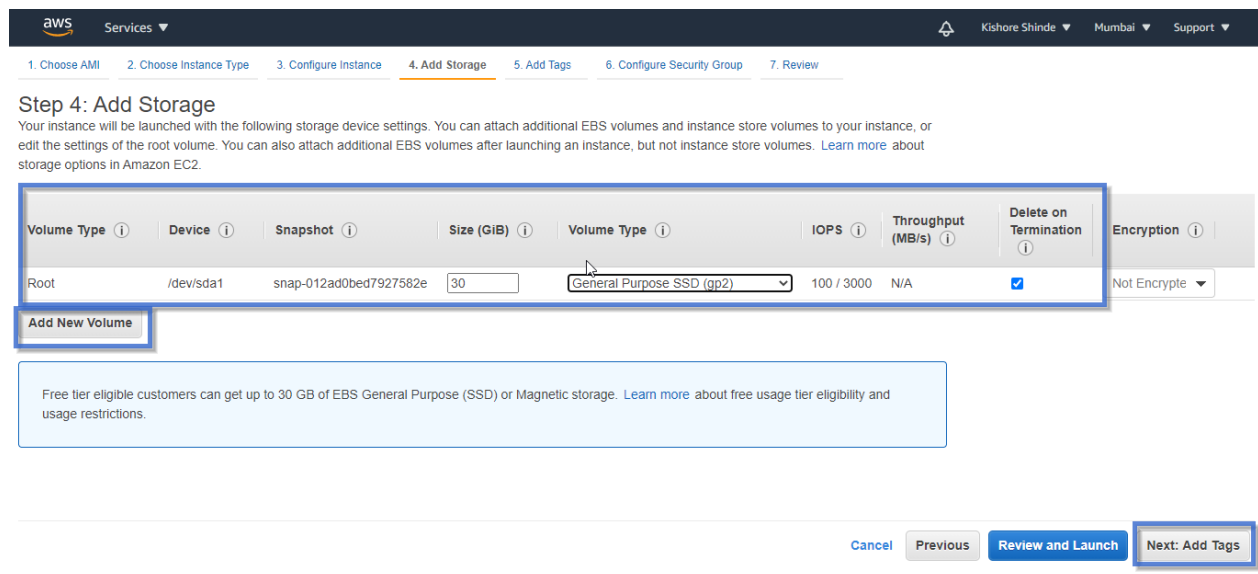
Enable termination protection: If you check it will protect your instance from accidental termination.



Now keep whatever is default don't change anything and click on Next: Add Storage

Step 4: Add Storage

Your Instance will be launched with the following storage device settings. You can attach additional EBS volumes. For now, keep the default Volume Type: Root and size: 30 GiB (only 30 GB is free for free tier for General purpose SSD) and General-Purpose SSD (gp2) as it is. Delete on Termination checkbox will make sure the volume gets deleted as soon as the Instance is terminated. You can even add new EBS volume. Click on Next: Add Tags



Step 5: Add Tags

Tags enable you to categorize your AWS resources in different ways. Each tag is a simple label consisting of customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. For E.g. Key can be Name and Value can be Web Server (With IIS).

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
Name	IIS Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

You can add the tag or can continue to next step “Configure Security Group”

Step 6: Configure Security Group

A security group is similar to firewall. Here you can set the rules that can control traffic for your instance. For the current instance in the Type select “All Traffic” and in Source select “Anywhere”. It will show you a warning that the source anywhere will allow all IP addresses to access your instance you must select IP Addresses only. Ignore it for now and click on “Review and Launch”.

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
All traffic	All	0 - 65535	Anywhere	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](#)

Step 7: Review

Here you can review all the selection you have done in previous steps and if required can go back and change them. You are able to review the AMI details, Instance Type/Details, Security Groups, Storage & Tags.

aws Services

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Improve your instances' security. Your security group, launch-wizard-16, 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](#)

AMI Details [Edit AMI](#)

Microsoft Windows Server 2019 Base - ami-0f438f5108b5217e
 Microsoft Windows 2019 Datacenter edition, [English]
 Root Device Type: ebs Virtualization type: hvm
 If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the License Mobility Form. [Don't show me this again](#)

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snp-012ad0bed7927582e	30	gp2	100 / 3000	N/A	Yes	Not Encrypted

[Cancel](#) [Previous](#) [Launch](#)

Click on Launch once you have reviewed all the details.

Next it will ask you to Select an existing key pair or create a new key pair.

Select an existing key pair or create a new key pair ✕

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.

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.](#)

Create a new key pair ▼

Key pair name
 WindowsIT

[Download Key Pair](#)

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.

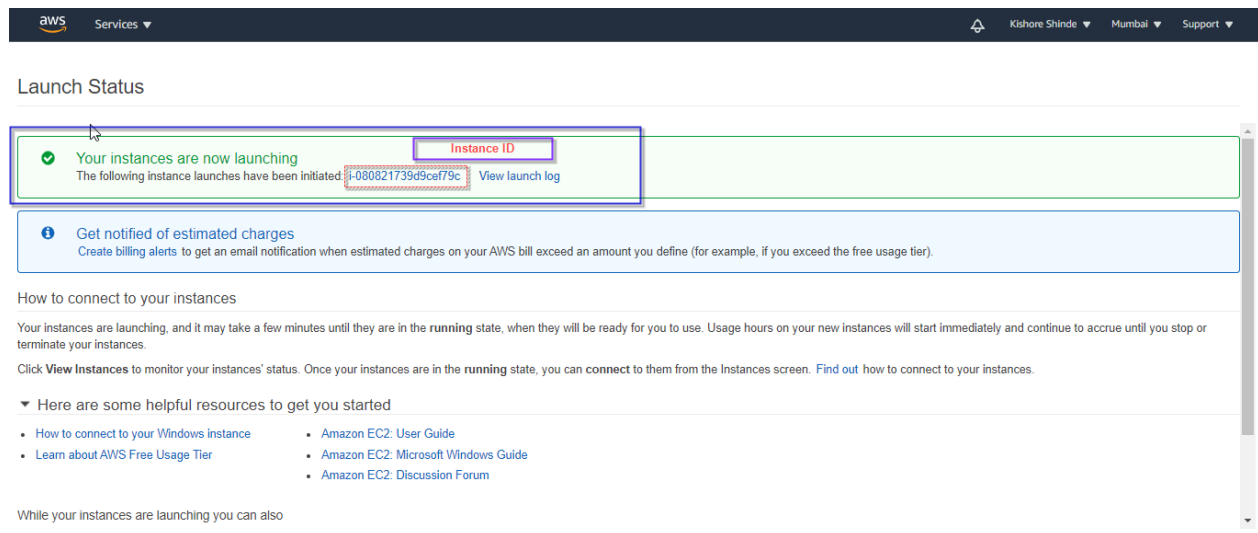
[Cancel](#) [Launch Instances](#)

You can select existing key pair if you have one. For now, select "Create new pair" give key pair a name and download the keypair

Note: Please keep it safe, it will be required to connect to the instance otherwise you can't.

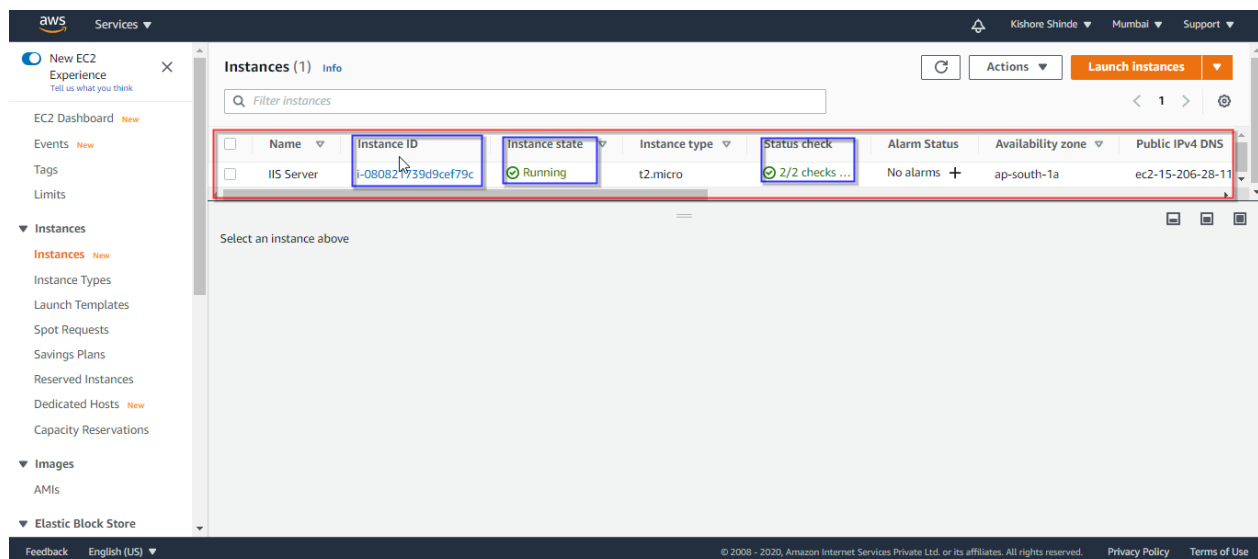
Click on Launch Instance.

In the next screen you will be able to see "Your instance is launching". You will be able to see the instance id that is initiated for launch.

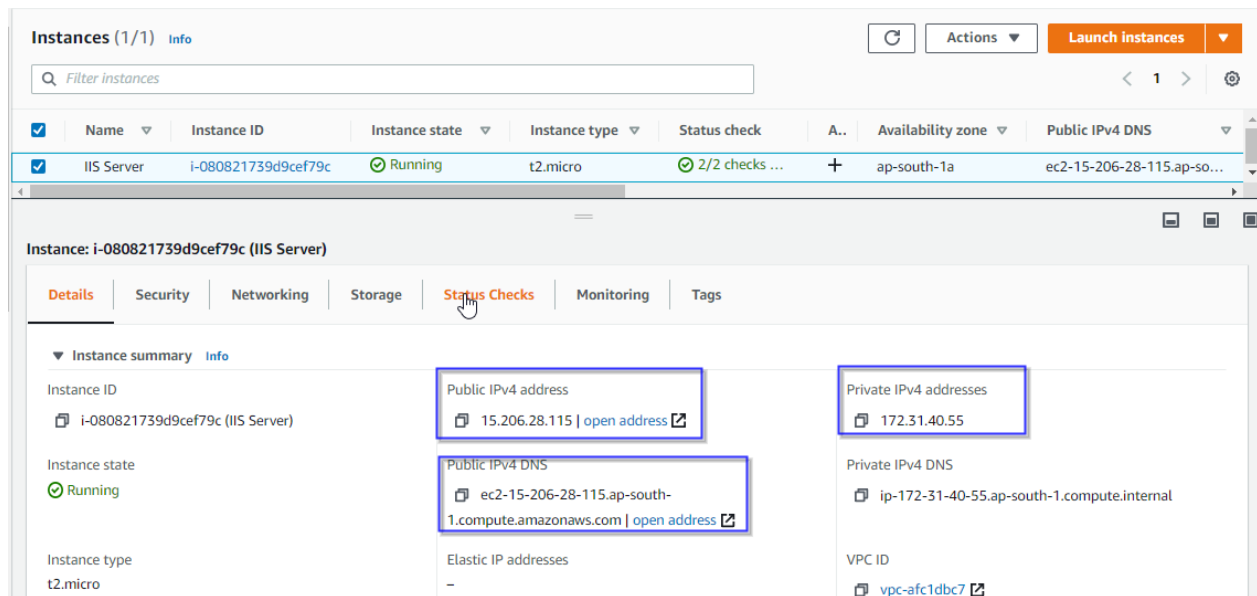


You can click on the instance id which will take you to Instances Dashboard.

Here you will see the instance created which will be initially showing Instance State as “Pending”. Wait till the Status check shows 2/2 checks and Instance State becomes “Running”.



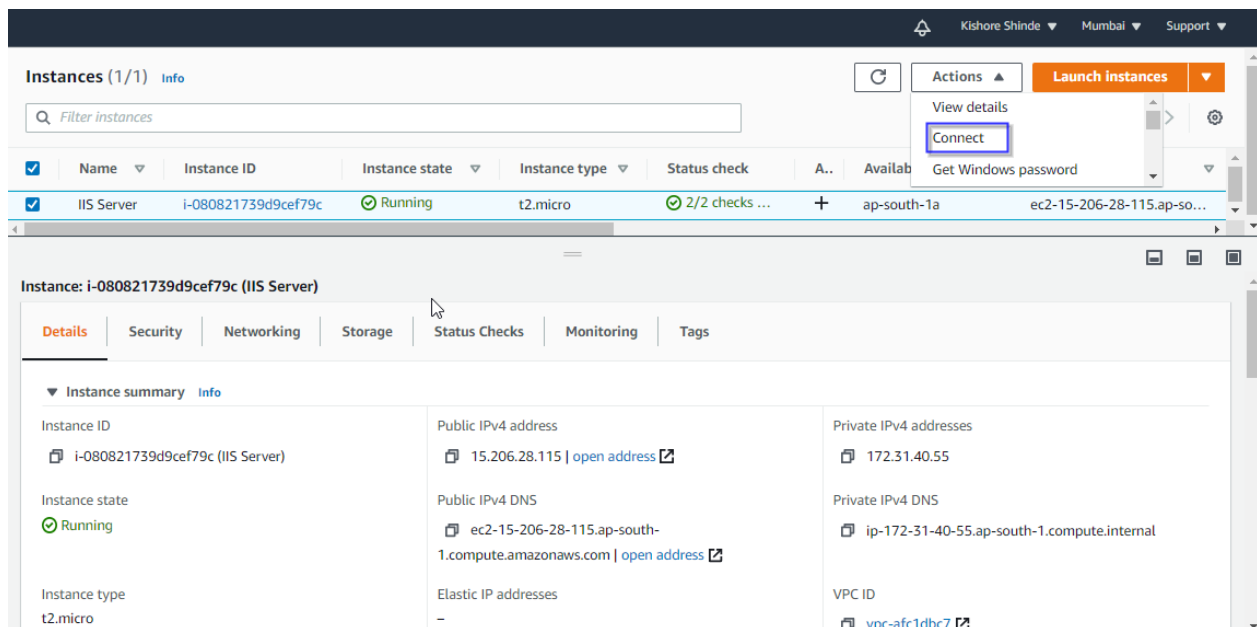
Now select the instance you will be able to see the additional details of the instance like Public IPv4 address, Private IPv4 address, Public IPv4 DNS, Private IPv4 DNS etc. You can also check the Security, Networking, Storage details etc.



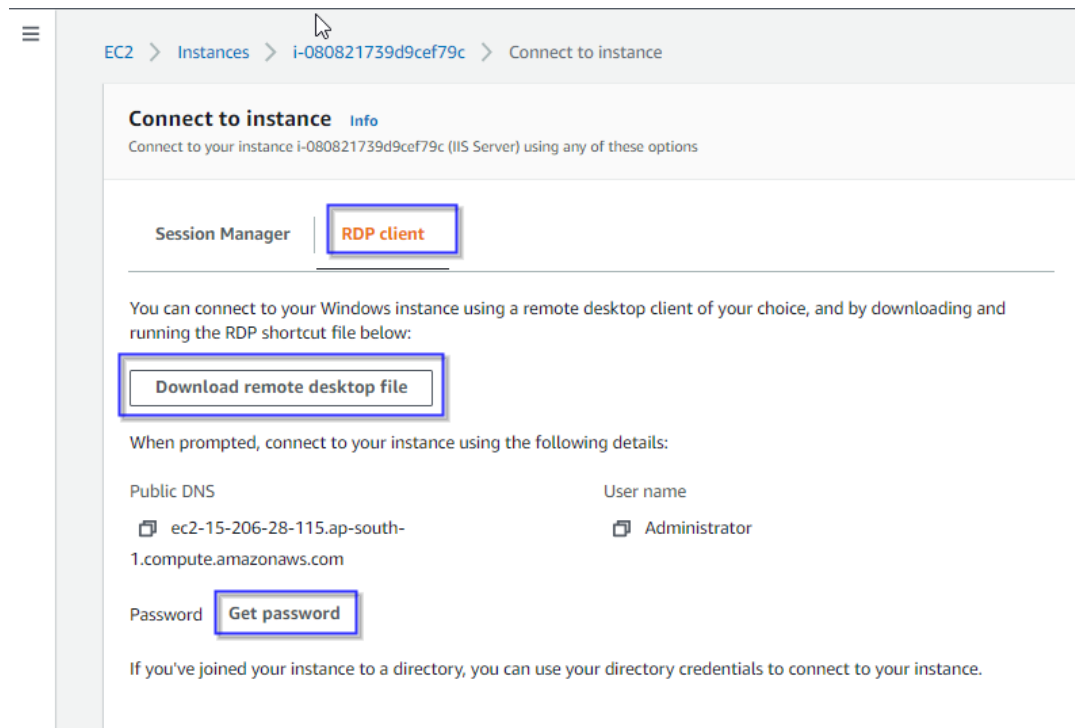
So now your instance is up and running.

Step B: Connecting to Windows Instance

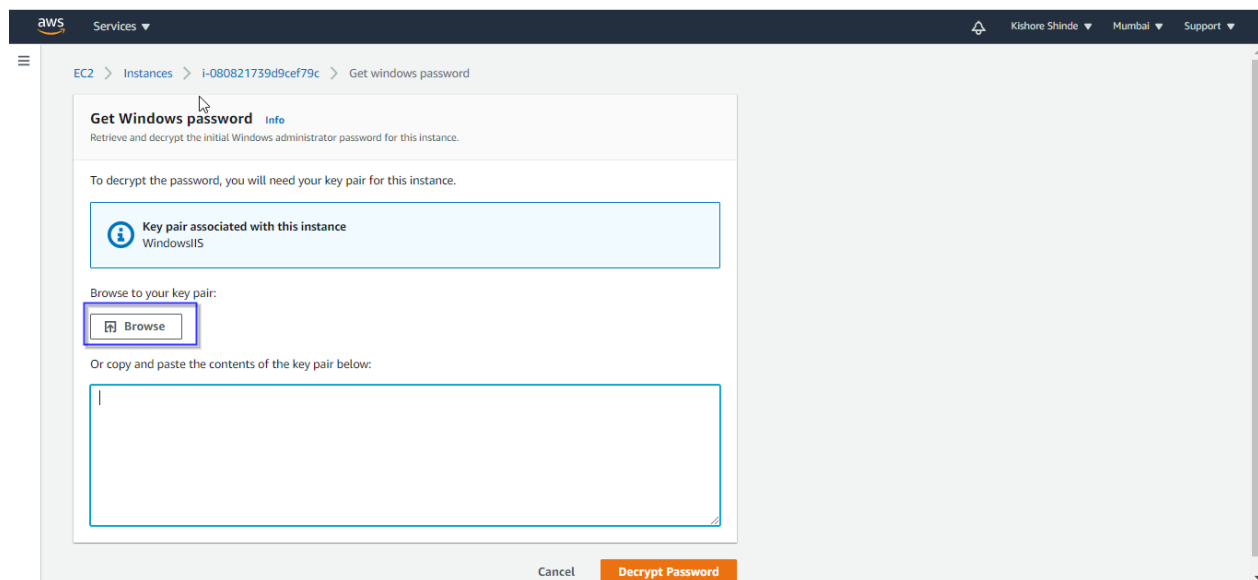
Following are the steps to connect to the instance. Select the instance, Click on Action menu at the top, from the list select Connect.



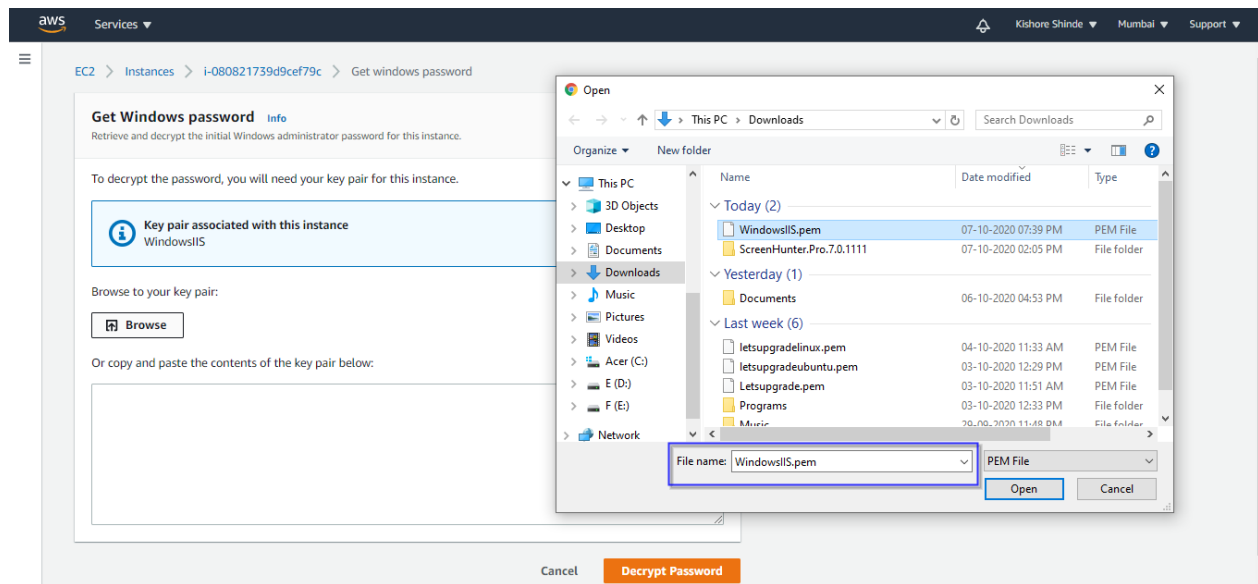
On the next screen you will see Session Manager & RDP Client Tabs. Click on RDP client.



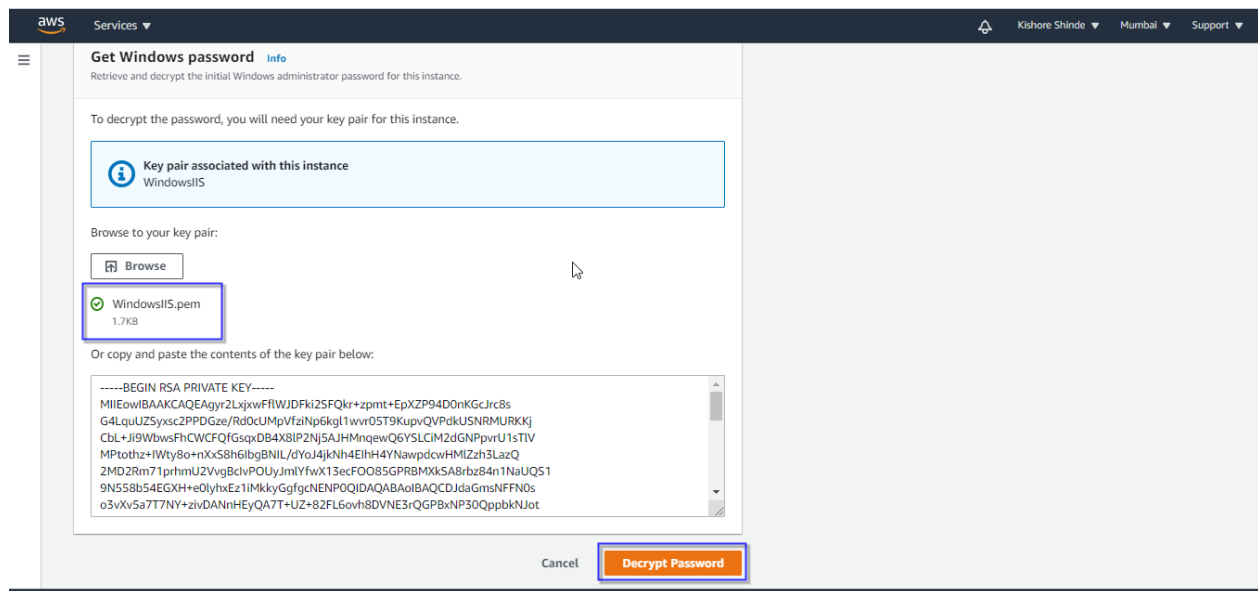
For accessing the instance, you will require RDP client. Click on “Download remote desktop file” & download the file. Now click on “Get password”



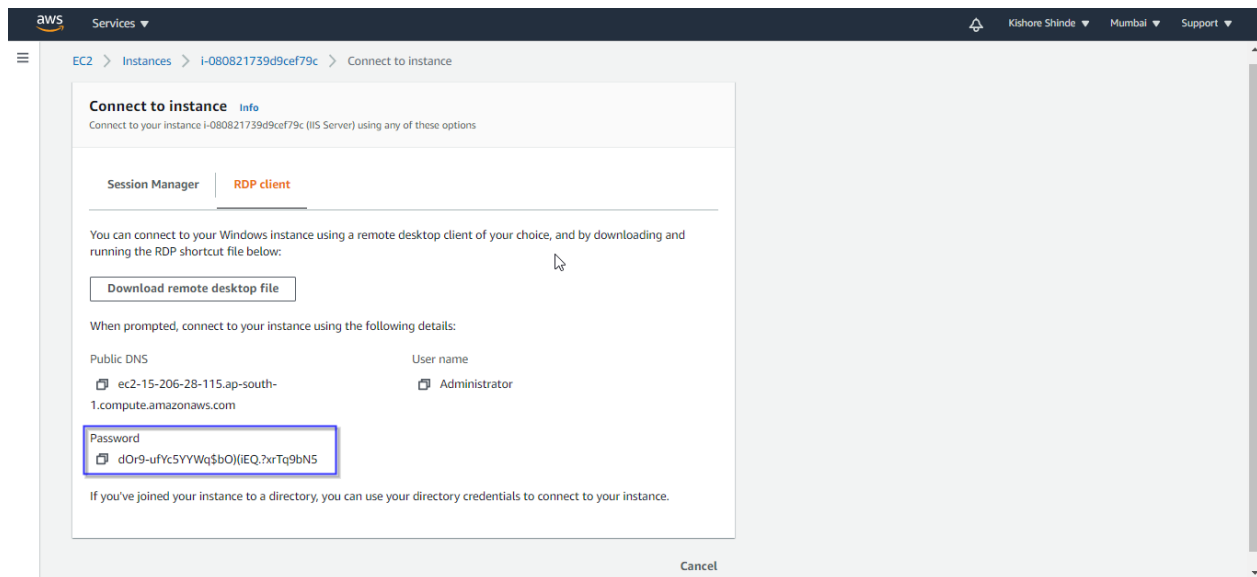
In the Get password screen select “Browse” to select the .pem file which you have downloaded after Step 7 in create key pair screen.



Select the file click on open.

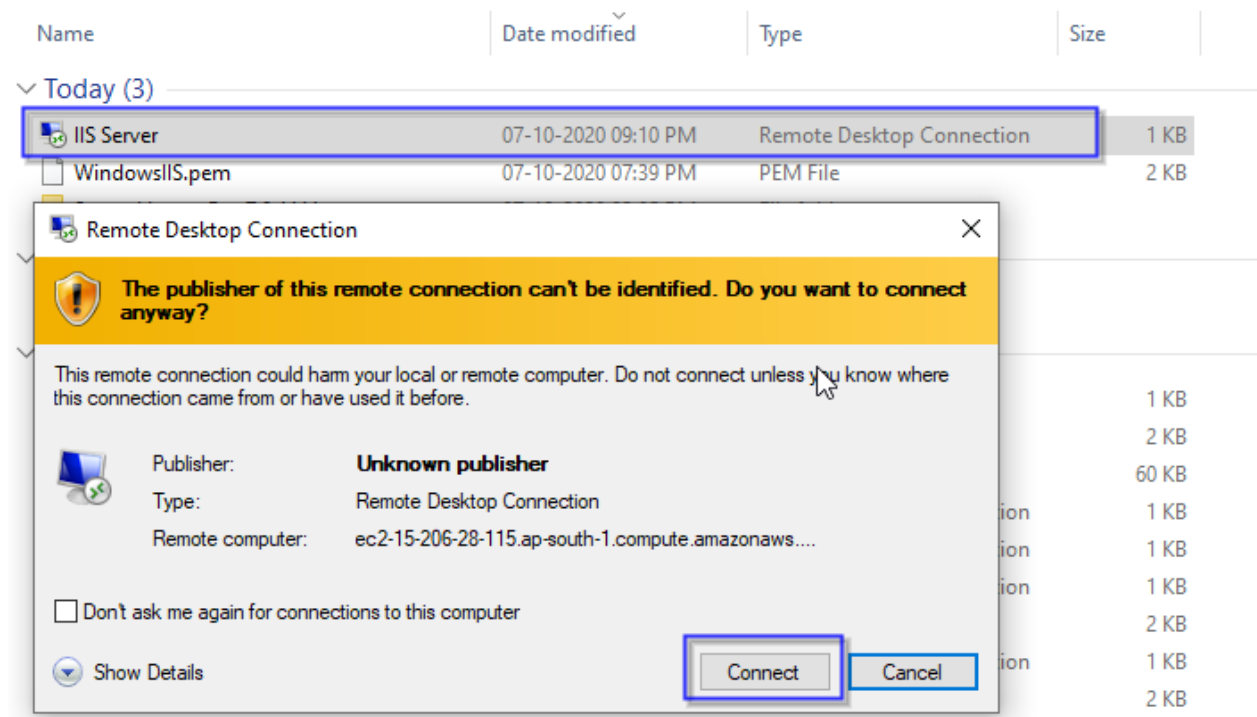


Click on "Decrypt Password".

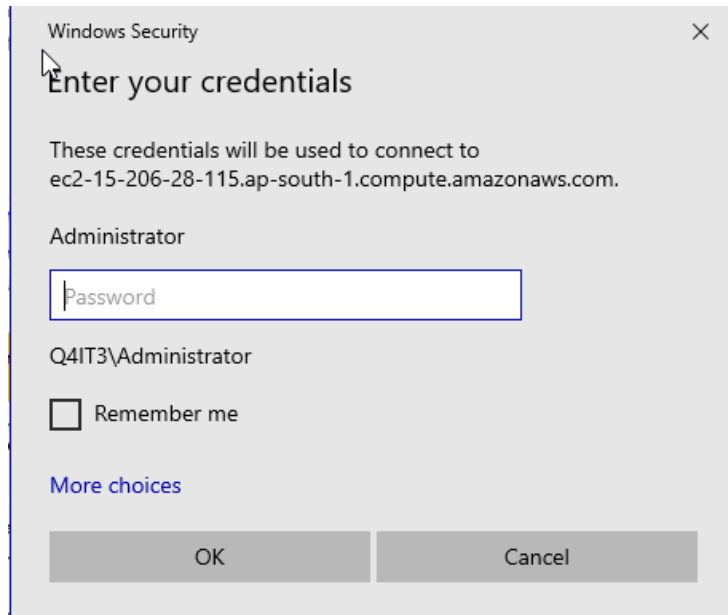


Copy the decrypted password similar to shown the above figure. This will be required when you connect the Instance through RDP client.

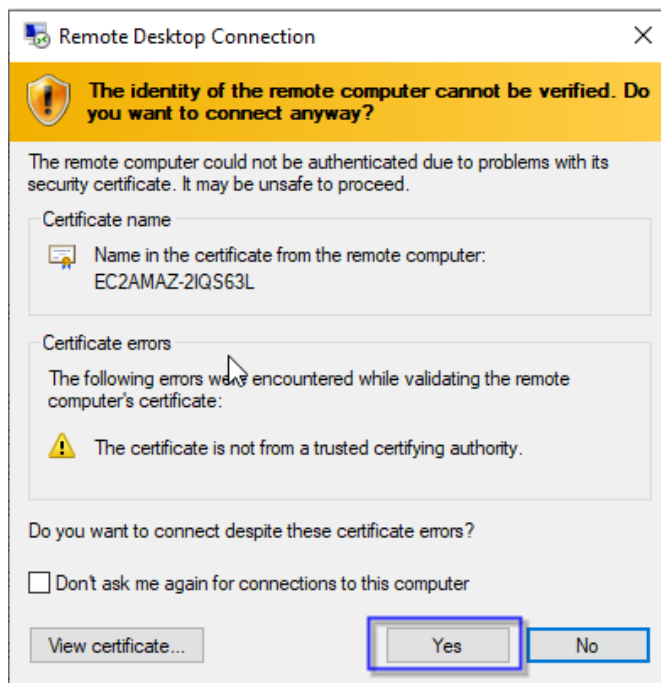
Now open the downloaded RDP client.



Click on Connect.



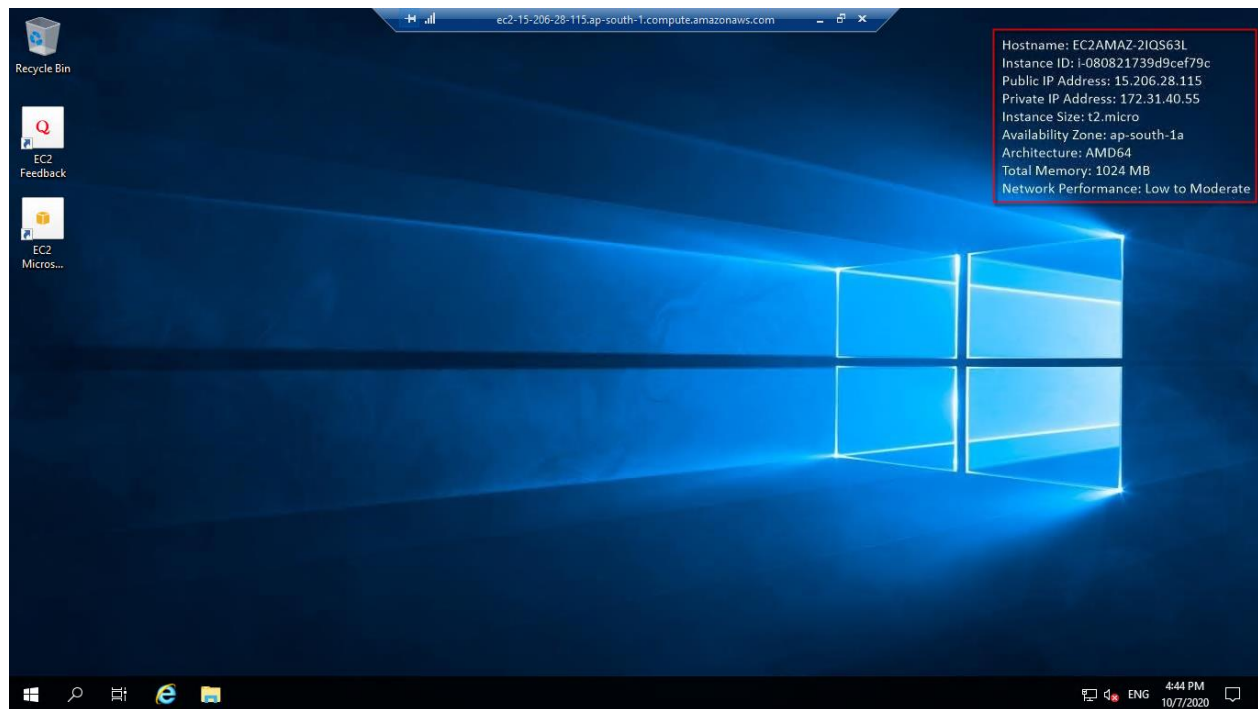
Enter or paste the password copied on the RDP client screen and click OK.



A Security Certificate error will be displayed but Click on Yes.

Now you will be connected to the instance. Wait for the settings to be done.

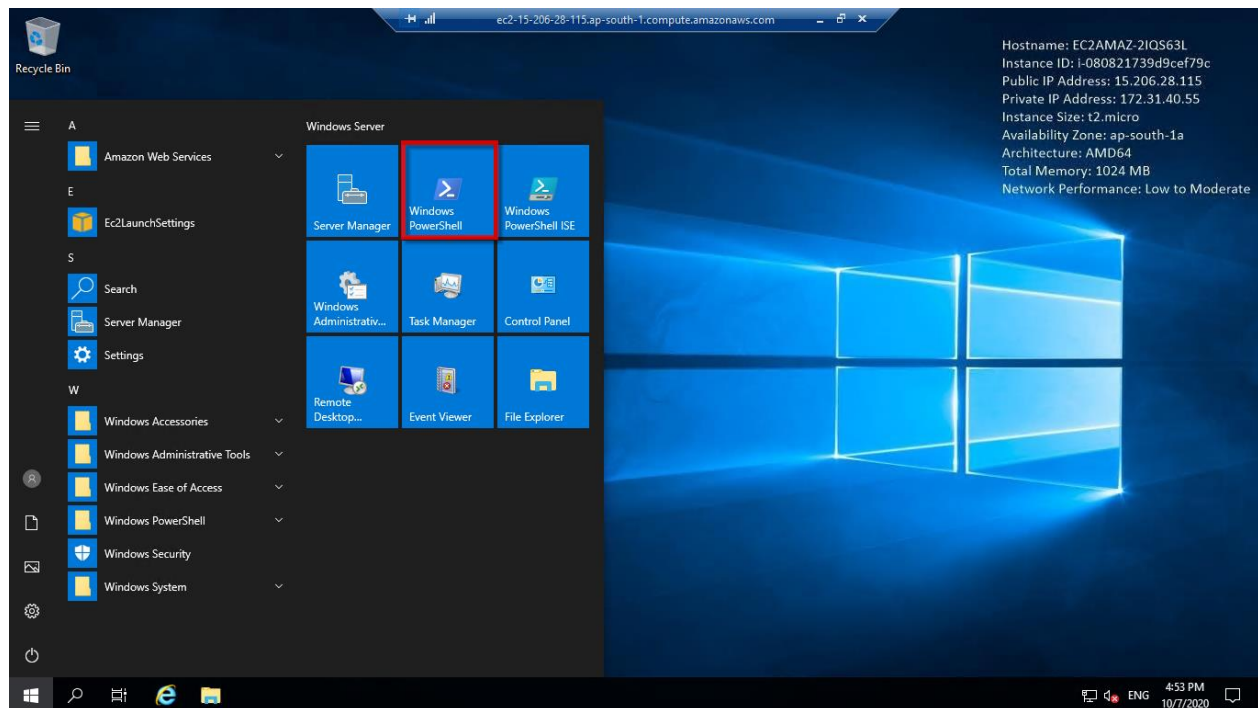
Once settings are done you will be able to see the Windows Server 2019 desktop with Instance details on the right side.



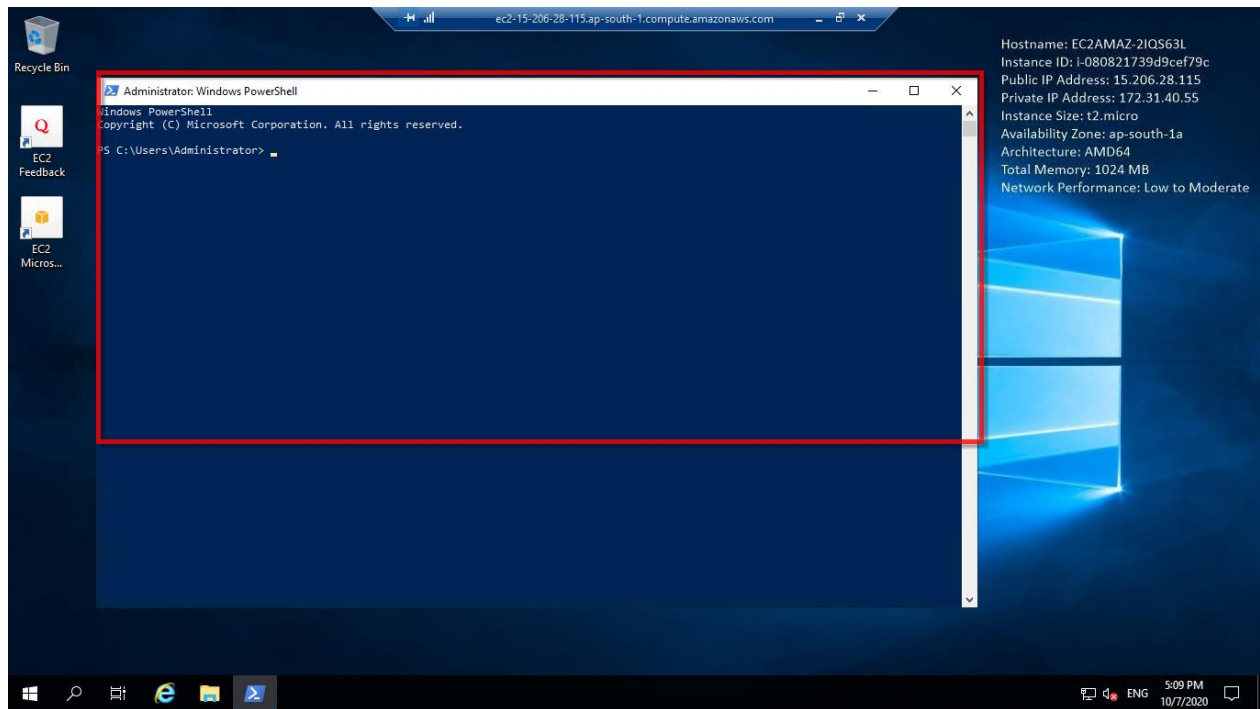
STEP C: Installing IIS

Below are the steps for installing IIS Server on Windows Server 2019 using PowerShell ISE.

Open Windows PowerShell

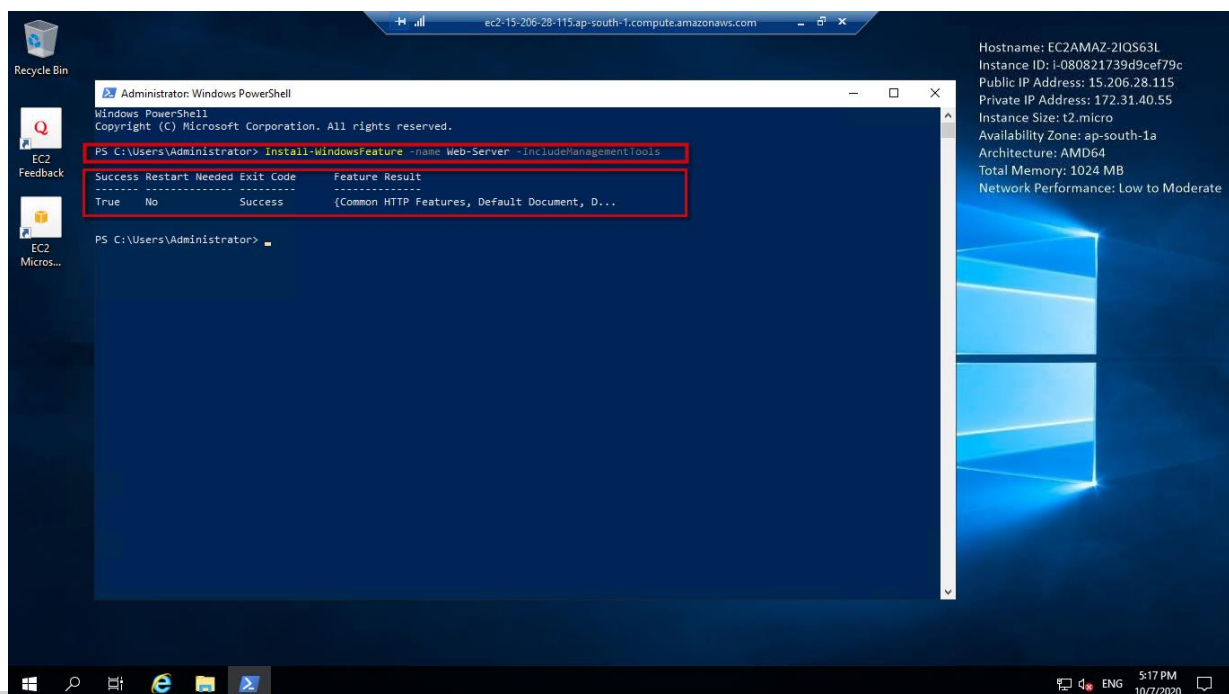


Below is the Windows PowerShell command prompt which opens with Administrator privileges/rights.

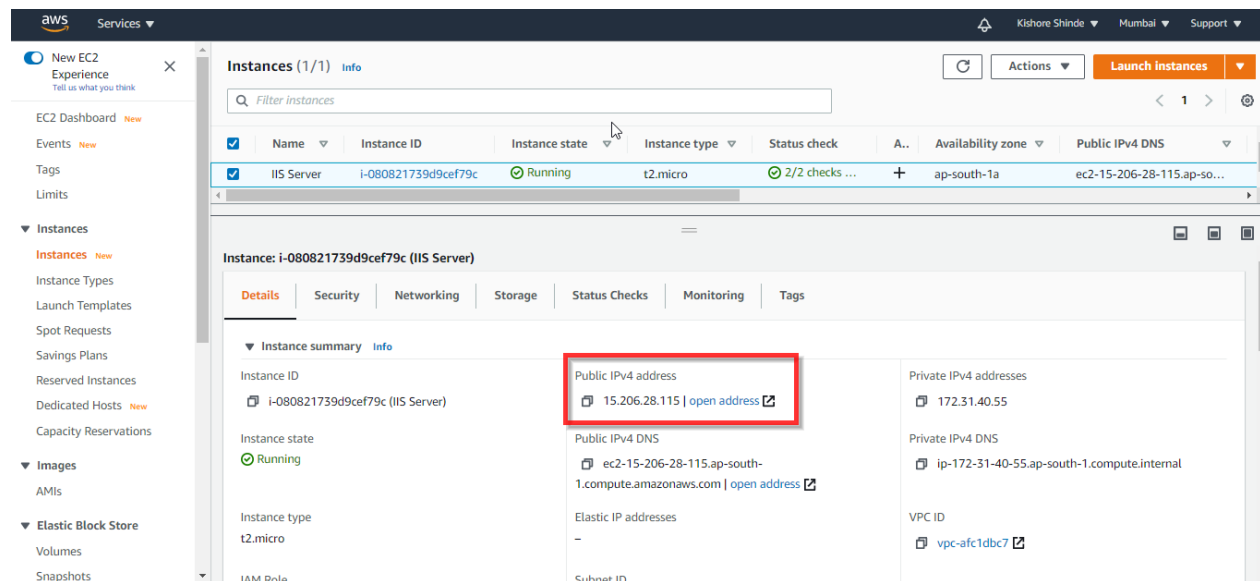


Type the below command to install the IIS Server.

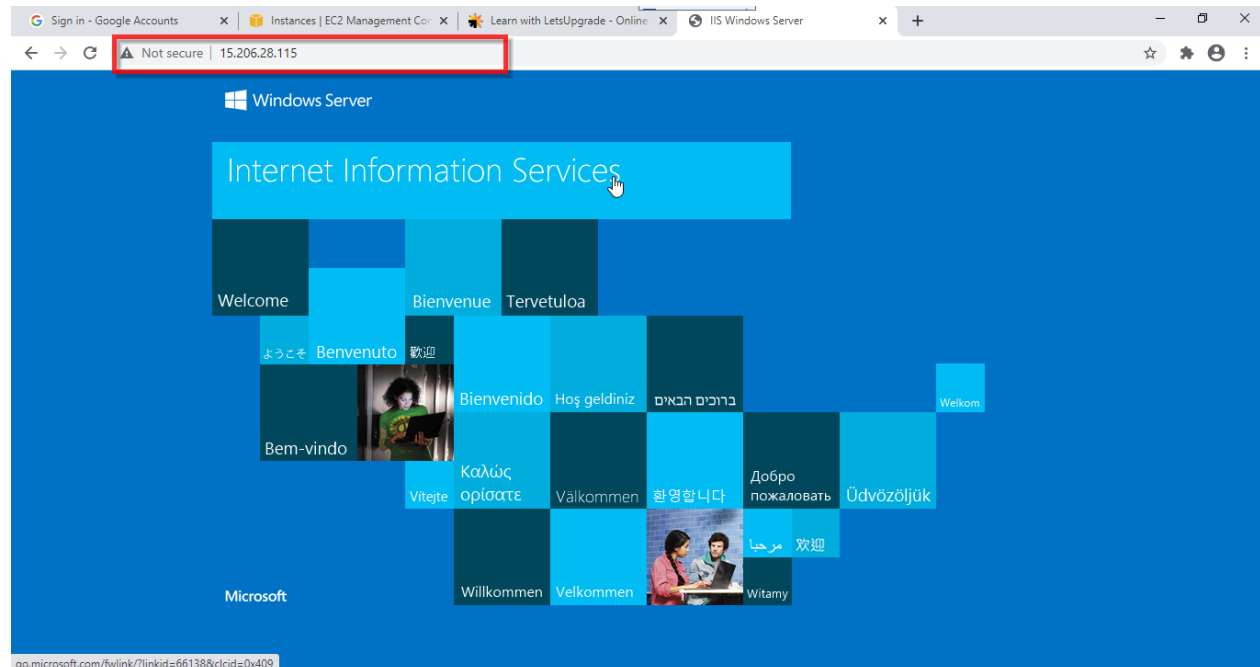
Install-WindowsFeature -name Web-Server -IncludeManagementTools & Press Enter to run the command. IIS will be downloaded & installed. Once installed you will see a Success – True. So, your IIS is installed.



Now to check the IIS Server installation. Copy the public address from the Instance details & paste it in your Internet browser (e.g. Chrome/Internet Explorer/Firefox) or click on open. In our current scenario our windows server public IP is: **15.206.28.115**

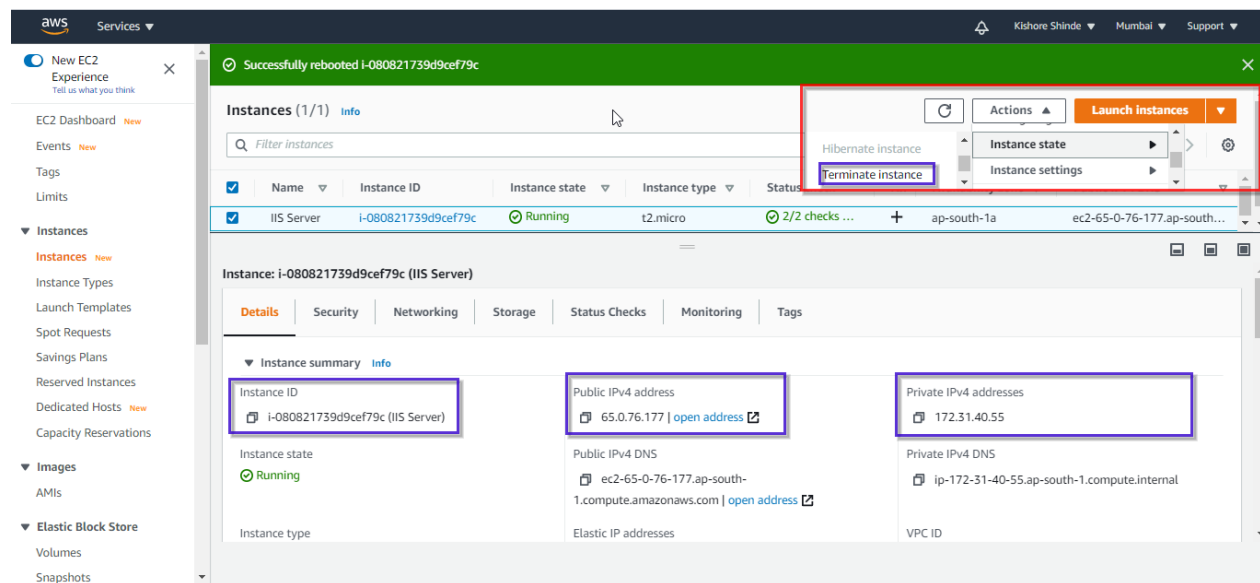


You should be able to see the IIS Server is deployed on the Windows Server 2019.

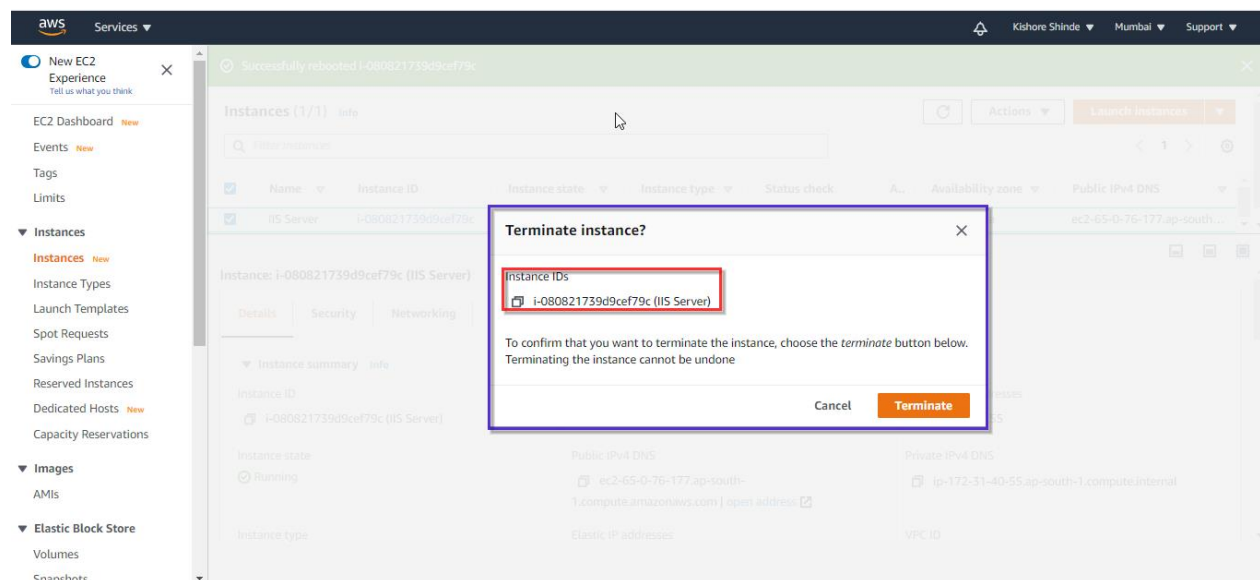


STEP D: Terminating Instance

Click on Actions->Select Instance State->Click on Terminate instance.



It will ask you for Termination permission click on Terminate.



The instance will be terminated and, in the instance, details you will see the public & private IP will be released which will go to shared pool and the instance status will show terminated.

aws Services

New EC2 Experience
Tell us what you think

EC2 Dashboard New

Events New

Tags

Limits

Instances

Instances New

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Snapshots

Successfully rebooted i-080821739d9cef79c

Successfully terminated i-080821739d9cef79c

Instances (1/1) Info

Filter instances

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	A..	Availability zone	Public IPv4 DNS
<input checked="" type="checkbox"/>	IIS Server	i-080821739d9cef79c	Terminated	t2.micro	2/2 checks ...	+	ap-south-1a	-

Instance: i-080821739d9cef79c (IIS Server)

Details Security Networking Storage Status Checks Monitoring Tags

Instance summary Info

Instance ID i-080821739d9cef79c (IIS Server)	Public IPv4 address -	Private IPv4 addresses -
Instance state Terminated	Public IPv4 DNS -	Private IPv4 DNS -
Instance type t2.micro	Elastic IP addresses -	VPC ID -

Project 1 is completed.