

VIRTUAL PRIVATE CLOUD WITH WINDOWS APPLICATION HOST:

Step1:create vpc

Step2:Create Subnet(public& private)

Step3:Create Internet Gateway And Attach Vpc

Step4:Create Public And Private Route Table

Step5: Subnet Association Add

Step6: Internet Gateway Add Success For Public and Private Route Table.

Step7: Nat Gateway For Only Public Route Table

Step8: Create Security Group For Public

Create Security Group---->Security Group Name(Public Security)----
>Vpc(Select Created Vpc)---->Inbound Rules--->1.Rdp---->Source(Anywhere)----
->2.HTTP----> Source(Anywhere)-----> Create Security Group..

Create security group [info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [info](#)
public security
Name cannot be edited after creation.

Description [info](#)
ssh

VPC [info](#)
vpc-0b3d7529f98a9981

Inbound rules [info](#)

Type	Protocol	Port range	Source	Description - optional
RDP	TCP	3389	Anywhere-IPv4	0.0.0.0
HTTP	TCP	80	Anywhere-IPv4	0.0.0.0

[Add rule](#)

Outbound rules [info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	0.0.0.0

[Add rule](#)

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Create security group](#)

Public Security Group Created...

Step9: Create Security Group For Private

Create Security Group---->Security Group Name(Privatesecurity)-----
>Vpc(Select Created Vpc)---->Inbound Rules--->All Tcp---->Source(Custom)-----
>Select Public Security Id(Public Security)---->create security group

The screenshot shows the 'Create security group' page in the AWS Management Console. The browser tabs include 'Launch an instance | EC2 Manag...', 'EC2 Management Console', and 'VPC Management Console'. The URL is 'ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreateSecurityGroup:'. The page title is 'Create security group'. Below the title, a note states: 'A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.'

Basic details

- Security group name:
- Description:
- VPC:

Inbound rules

Type	Protocol	Port range	Source	Description - optional
All TCP	TCP	0 - 65535	Custom	
<input type="text" value="sg-0181ee44a24dd09d9"/>				<input type="button" value="Delete"/>

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	
<input type="text" value="0.0.0.0"/>				<input type="button" value="Delete"/>

Tags - optional

No tags associated with the resource.

Step10: Public Ec2 Windows Instance Create:

The screenshot shows the 'Launch instance' page in the AWS Management Console. The page is divided into several sections:

- Instance type**: t2.micro, Free tier eligible, Compare instance types.
- Key pair (login)**: Key pair name - required: . .
- Network settings**:
 - VPC - required: . .
 - Subnet: . .
 - Auto-assign public IP: ☒ Enable.
- Firewall (security groups)**:
 - ☐ Create security group.
 - ☒ Select existing security group.
 - Common security groups: . .

Summary

- Number of instances:
- Software Image (AMI): Amazon Linux 2 Kernel 5.10 AML...read more
- Virtual server type (instance type): t2.micro
- Firewall (security group): public security
- Storage (volumes): 1 volume(s) - 8 GiB

Step11: Private Ec2 Windows Instance Create:

the instance.

Key pair name - *required*

mum1358 [Create new key pair](#)

▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0b3d75297f98af981 (myvpc1)
10.0.0.0/16

Subnet [Info](#)

subnet-03e4fab6c6f2449f private subnet
VPC: vpc-0b3d75297f98af981 Owner: 795071115491
Availability Zone: ap-south-1b IP addresses available: 250 CIDR: 10.0.2.0/24

[Create new subnet](#)

Auto-assign public IP [Info](#)

Disable

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

Common security groups [Info](#)

Select security groups

private security sg-029235d931bafbd1f1 [X](#)
VPC: vpc-0b3d75297f98af981

[Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

[► Advanced network configuration](#)

▼ Configure storage [Info](#) [Advanced](#)

1x 8 GiB gp2 Root volume (Not encrypted)

[Free tier eligible customers can get up to 30 GB of EBS General Purpose \(SSD\) or Magnetic storage](#) [X](#)

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-0cca134ec43cf708f

Virtual server type (instance type)
t2.micro

Firewall (security group)
private security

Storage (volumes)
1 volume(s) - 8 GiB

[Cancel](#) [Launch instance](#)

Step12: instance created

Launch an instance | EC2 Manag... | Launch an instance | EC2 Manag... | EC2 Management Console | Instances | EC2 Management Co... |

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances?v=3;\$case=tags:true%\$C,client:false;\$regex=tags:false%\$C,client:false

Instances (1/4) [Info](#)

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring	Security group name	Key p...
public instance2	i-0c19ba35688af96d	Terminated	t2.micro	...	No alarms	ap-south-1a	disabled	mum	
private instance2	i-0a3d70d198a0e823	Terminated	t2.micro	...	No alarms	ap-south-1a	disabled	mum	
public	i-0828d1c90725f2fa0	Running	t2.micro	2/2 checks pass	No alarms	ap-south-1a	65.2.33.116	disabled	public security	mum
private	i-091c5c5460e052b2	Running	t2.micro	2/2 checks pass	No alarms	ap-south-1b	disabled	private security	mum

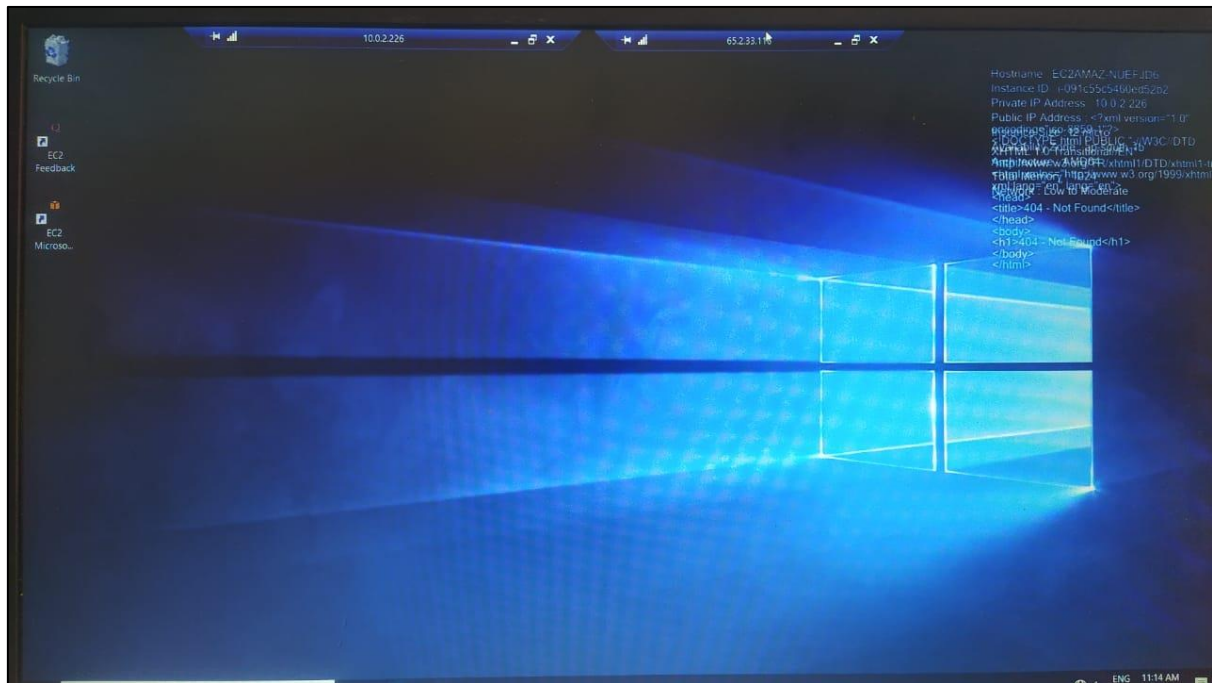
Instance: i-0828d1c90725f2fa0 (public)

[Details](#) [Security](#) [Networking](#) [Storage](#) [Status checks](#) [Monitoring](#) [Tags](#)

▼ Instance summary [Info](#)

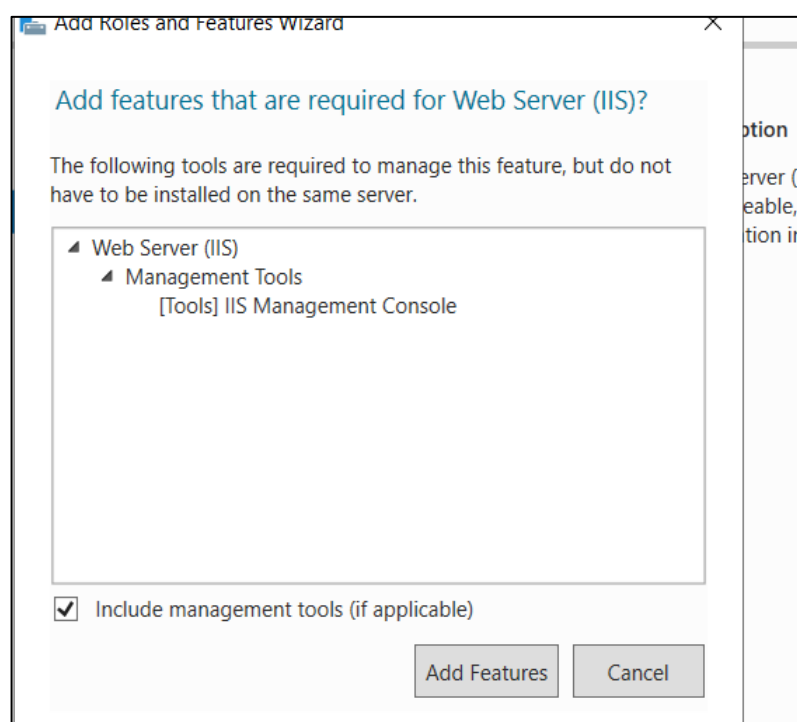
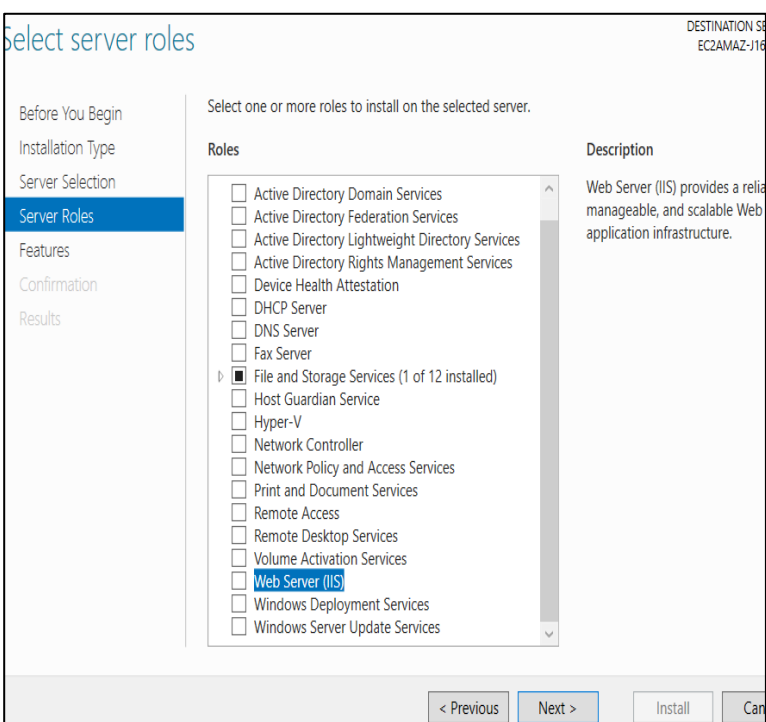
Instance ID	i-0828d1c90725f2fa0 (public)	Public IPv4 address	65.2.33.116 open address	Private IPv4 addresses	10.0.1.86
IPv6 address	...	Instance state	Running	Public IPv4 DNS	...
Hostname type	IP name: ip-10-0-1-86-ap-south-1-compute.internal	Private IP DNS name (IPv4 only)	ip-10-0-1-86-ap-south-1-compute.internal	Elastic IP addresses	...
Answer private resource DNS name	IPv4 (A)	Instance type	t2.micro	AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendation
Auto-assigned IP address	65.2.33.116 (Public IP)	VPC ID	vpc-0b3d75297f98af981 (myvpc1)	Auto Scaling Group name	...
IAM Role	...	Subnet ID	subnet-002986aa748c7740 (public subnet)	Monitoring	disabled
▼ Instance details Info	Platform	AMI ID	ami-0a070b85c12b8db0	Termination protection	Disabled
Platform details	Windows	AMI name	Windows_Server-2022-English-Full-Base-2022.12.14	AMI location	...
Stop protection	...	Launch time	...		

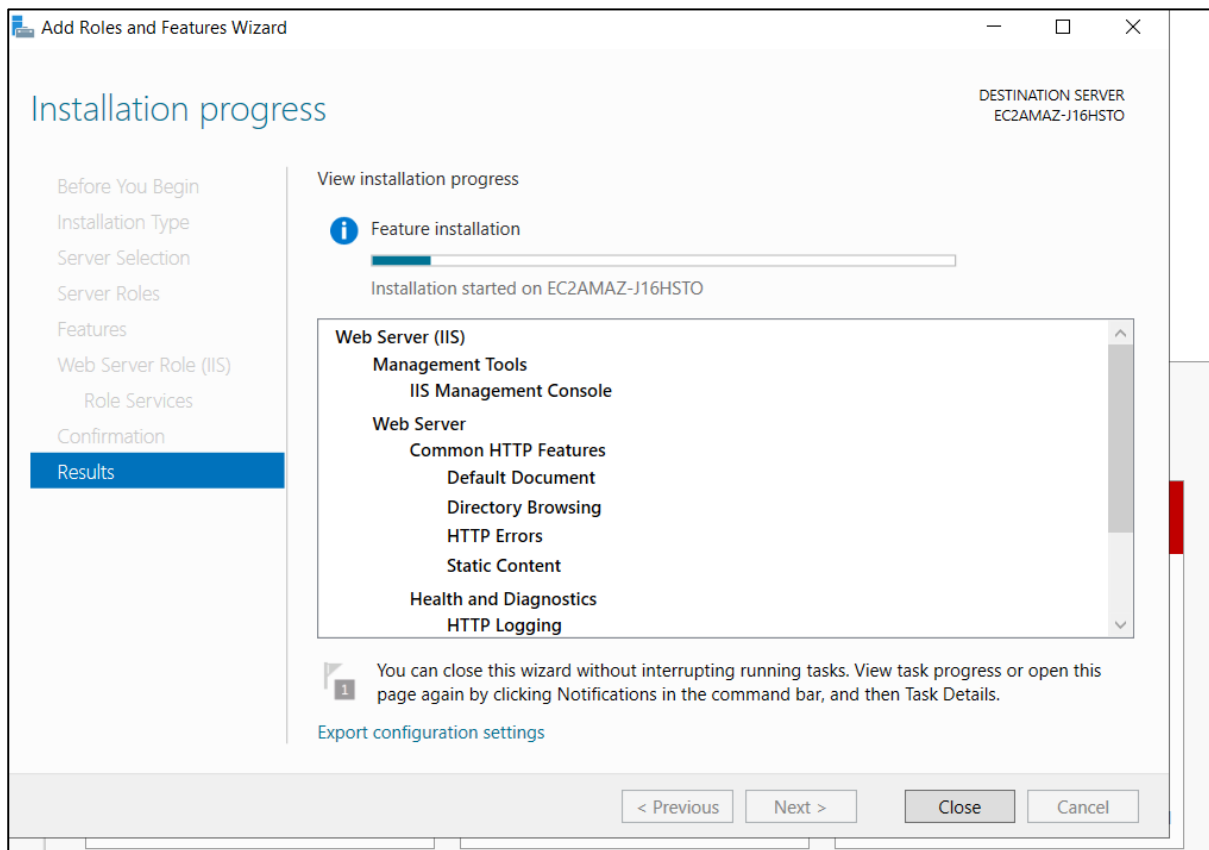
Step12:Open Instance Windows---->remote desktop connection--->put private instance private ip--->put username&password--->connect--->private windows instance open



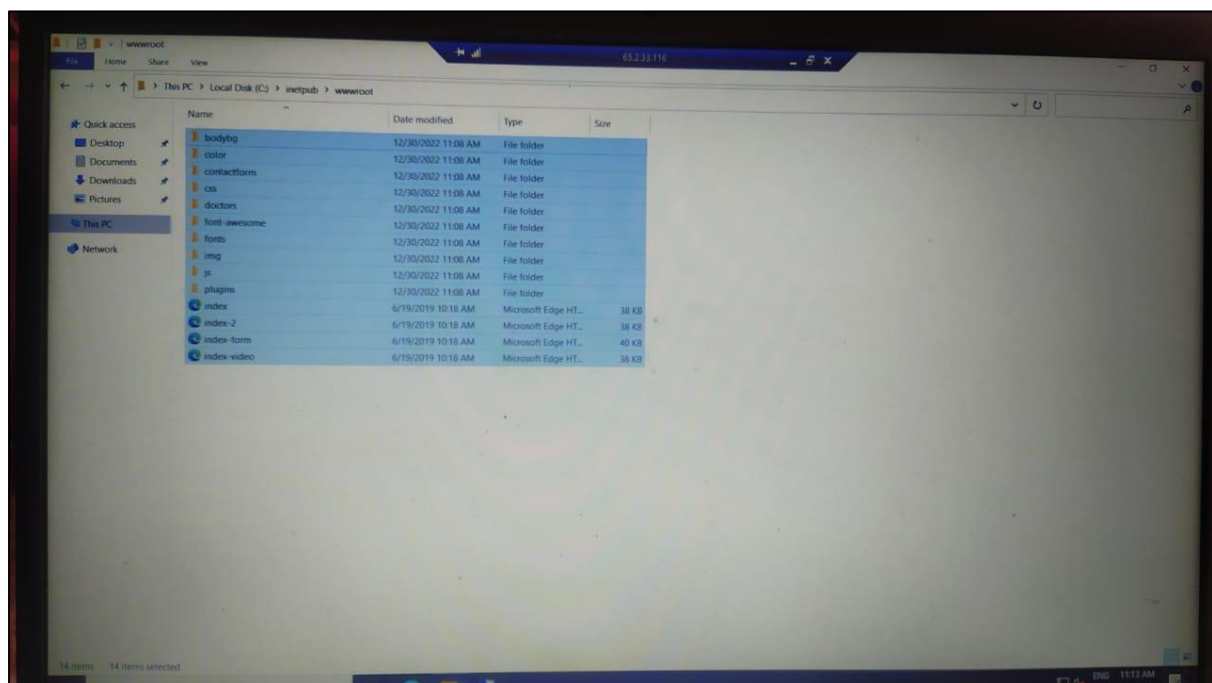
Two windows created instance (public & private) created.

Step13:Public Windows--->Server Manager--->Install IIS(internet information service)

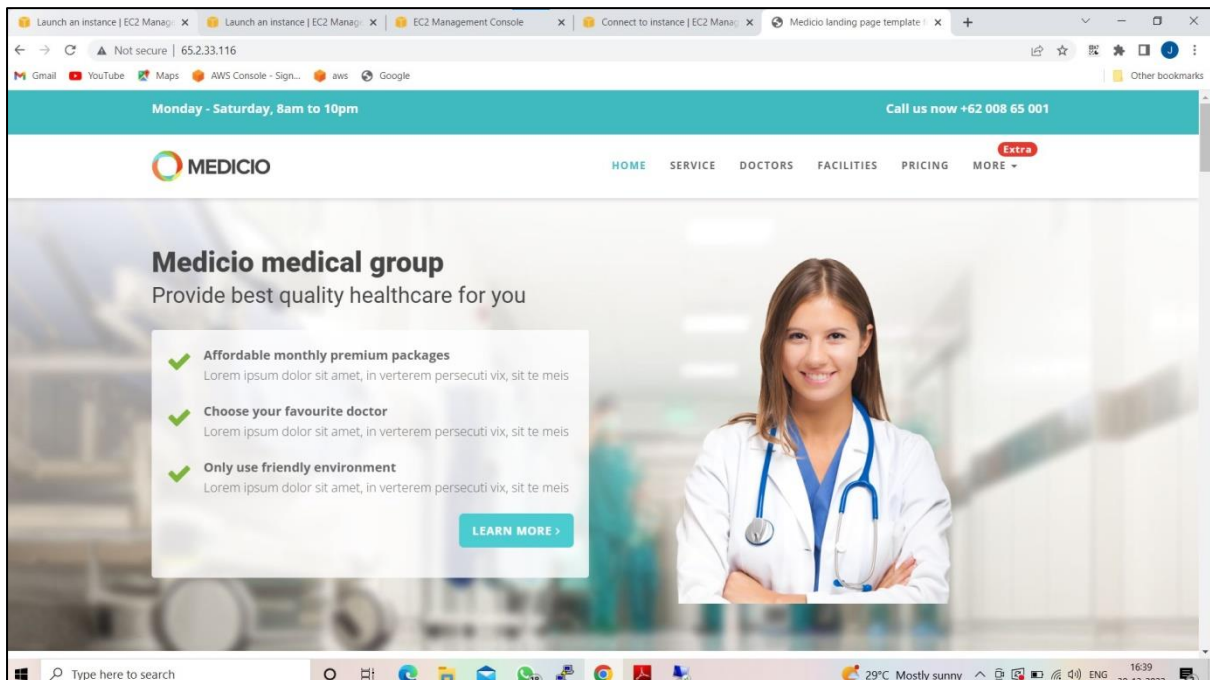




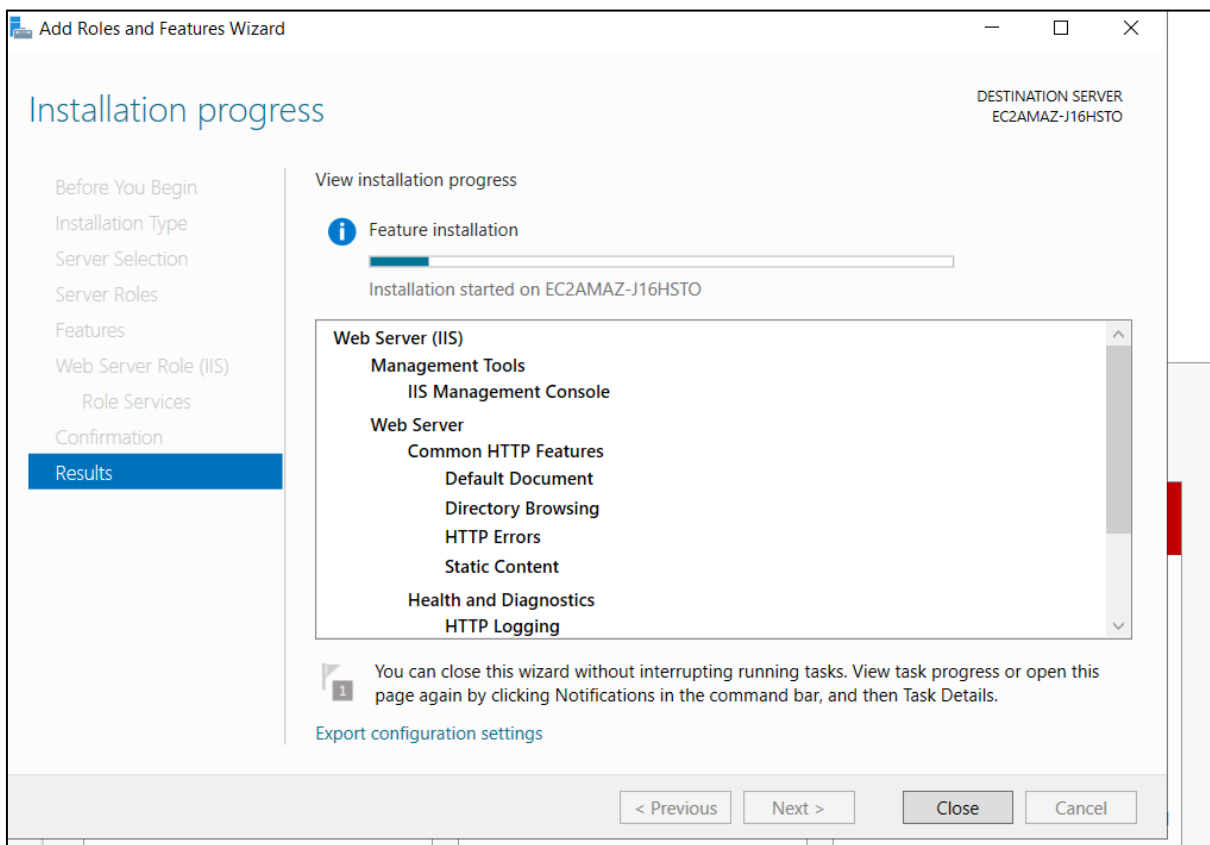
Step13.1:Copy Any Content--->Put C/Drive---->Inetpub--->Wwwroot



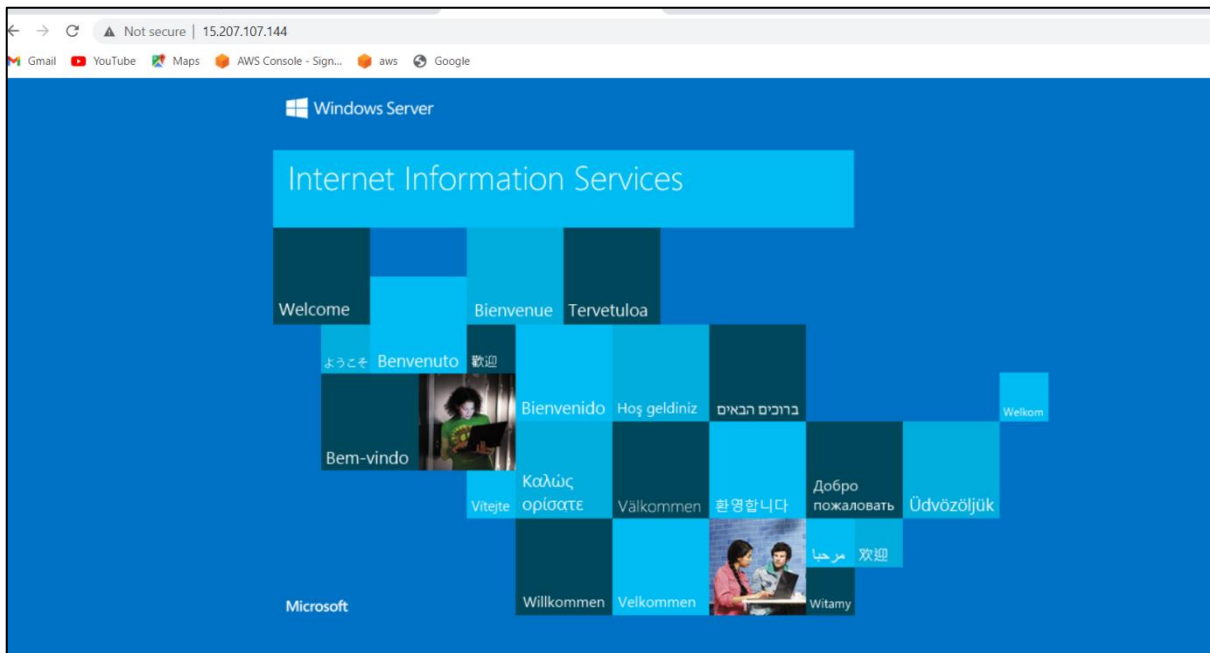
Step13.2:Copy Public Ip For Public Windows Instance---->Put Chrome(Show The Content Page)



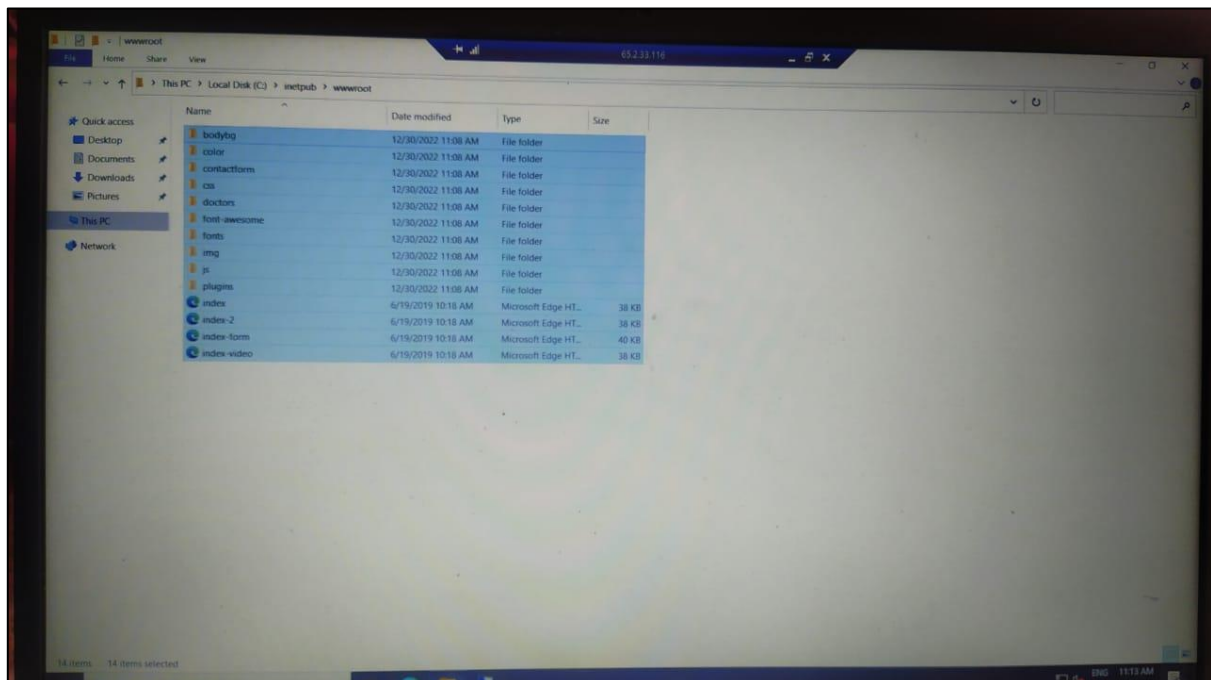
Step14:Private Windows--->Server Manager--->Install IIS(internet information service)



Step14.1:Copy Private Ip For Private Instance And Put Public Instance Microsoft Edge Text Page



Step14.2: Copy Any Content--->Put C/Drive---->Inetpub--->Wwwroot



Step14.3:Refresh Microsoft Edge Text Page --->Show Original Content Image

