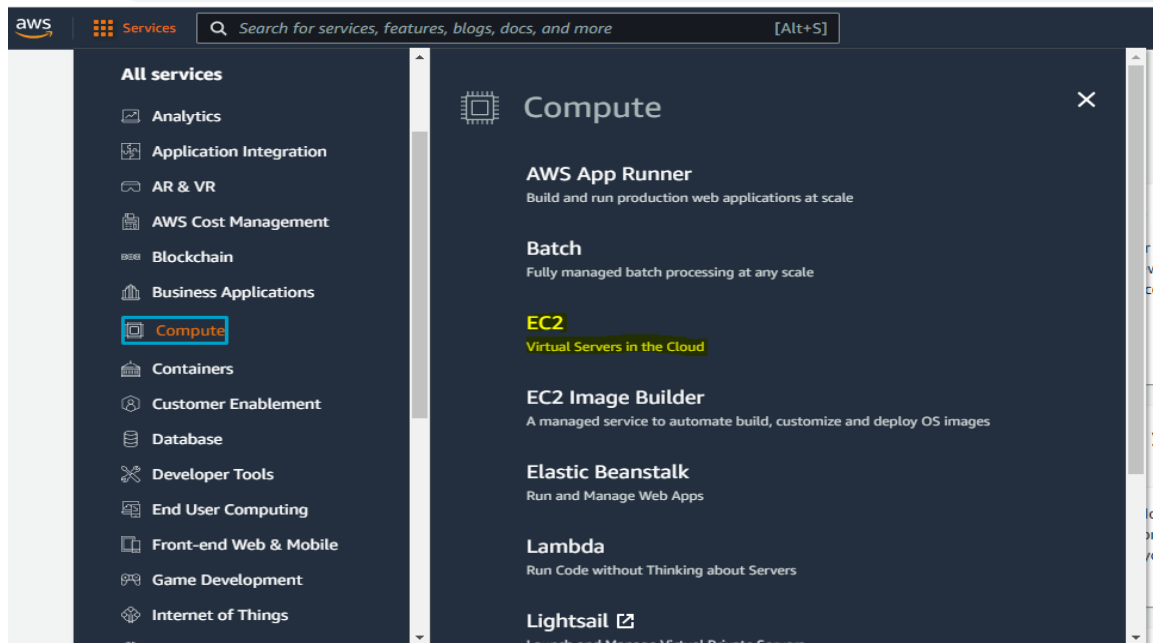


How to create an EC2 Linux machine and windows Machine :

Linux:::::::

Step 1:

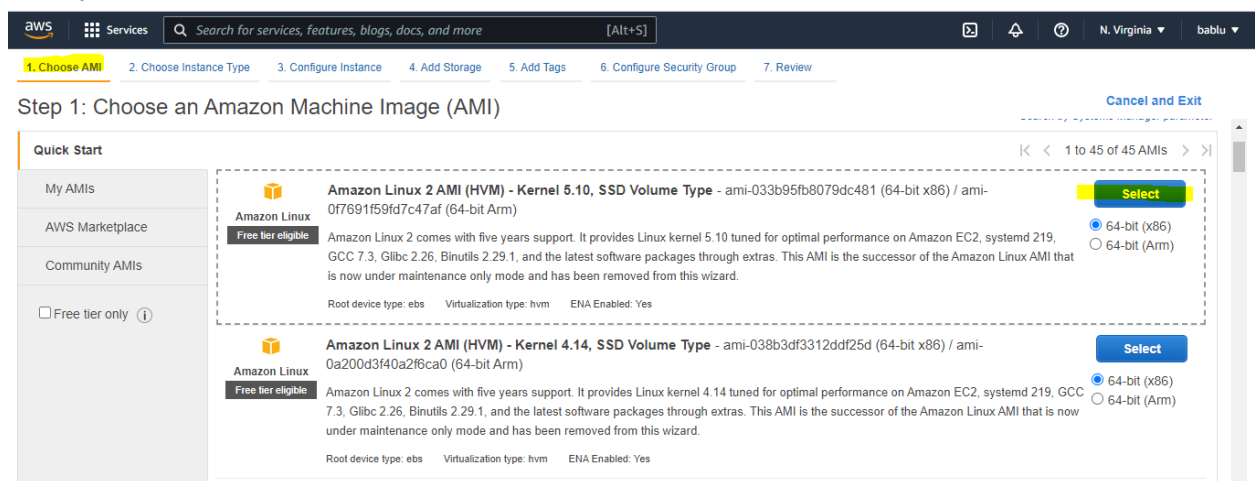
Click on all services and click on compute services and select EC2



Step2:

Click on launch instances

Then you see choose an ami



Step 3:

choose an instance based on your priority to launch the instances

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

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes

Here we can increase instances and create a vpc with subnets

“ If you don't specify anything it make takes the default one”

Number of instances ⓘ [Launch into Auto Scaling Group](#) ⓘ

Network ⓘ vpc-2f0c7152 (default) ↕ ↻ Create new VPC

Subnet ⓘ No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP Use subnet setting (Enable)

Hostname type ⓘ Use subnet setting (IP name) ⚙

DNS Hostname ⓘ

- ☒ Enable IP name IPv4 (A record) DNS requests
- ☒ Enable resource-based IPv4 (A record) DNS requests
- ☐ Enable resource-based IPv6 (AAAA record) DNS requests

Placement group ⓘ ☐ Add instance to placement group

Storage we can increase the 8gb but we can't decrease the size

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	/dev/xvda	snap-0e8a7a7609c630051	18	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
Add New Volume								
<p>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.</p>								
<p>Shared file systems ⓘ</p>								

Step 5:

We need to specify the “name” value should be the name of server.

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	Value	Instances	Volumes	Network Interfaces
Name	jenkins	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

Step6:

Security group name we can choose new one or we can create the existing one

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
SSH	TCP	22	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.

Step 7:

Atlast, we can review it and if any changes are necessary we can edit or else click on the launch .

Step 7: Review Instance Launch

eligible software packages through extras. This AMI is the successor of the **Amazon Linux AMI** that is n...
Root Device Type: ebs Virtualization type: hvm

Instance Type

[Edit instance type](#)

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

Security Groups

[Edit security groups](#)

Security group name: launch-wizard-24
Description: launch-wizard-24 created 2022-02-23T18:36:22.838+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

Instance Details

[Edit instance details](#)

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

After that it shows a pop-up to download the pem file click on the download key pair it may store in your local

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. Amazon EC2 supports ED25519 and RSA key pair types.

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 type

☒ RSA ☐ ED25519

Key pair name

bablu

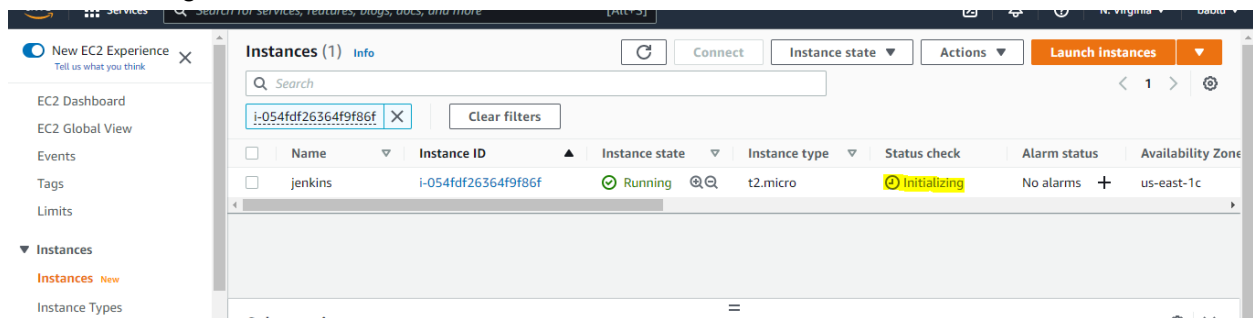
Download Key Pair



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.

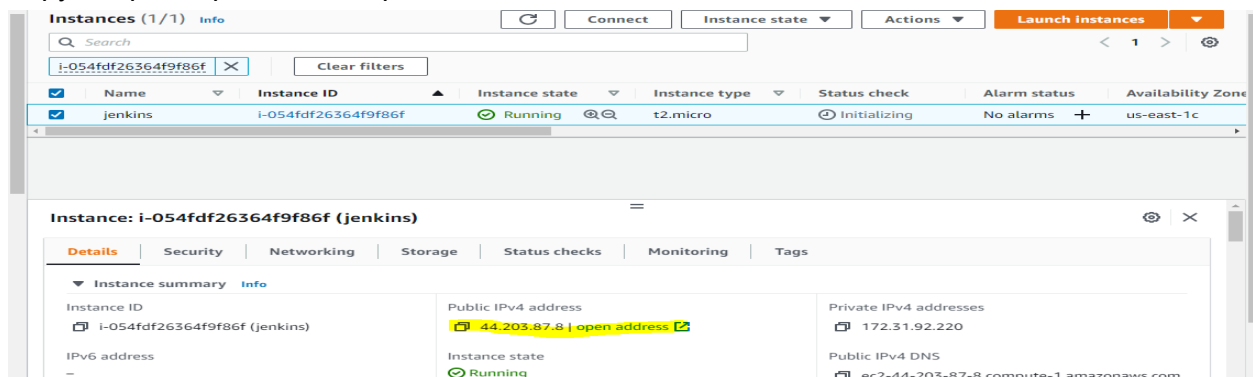
step8:

After this you can see the virtual server running on particular region and the status check shows from initializing to 2/2 checks



Step9:

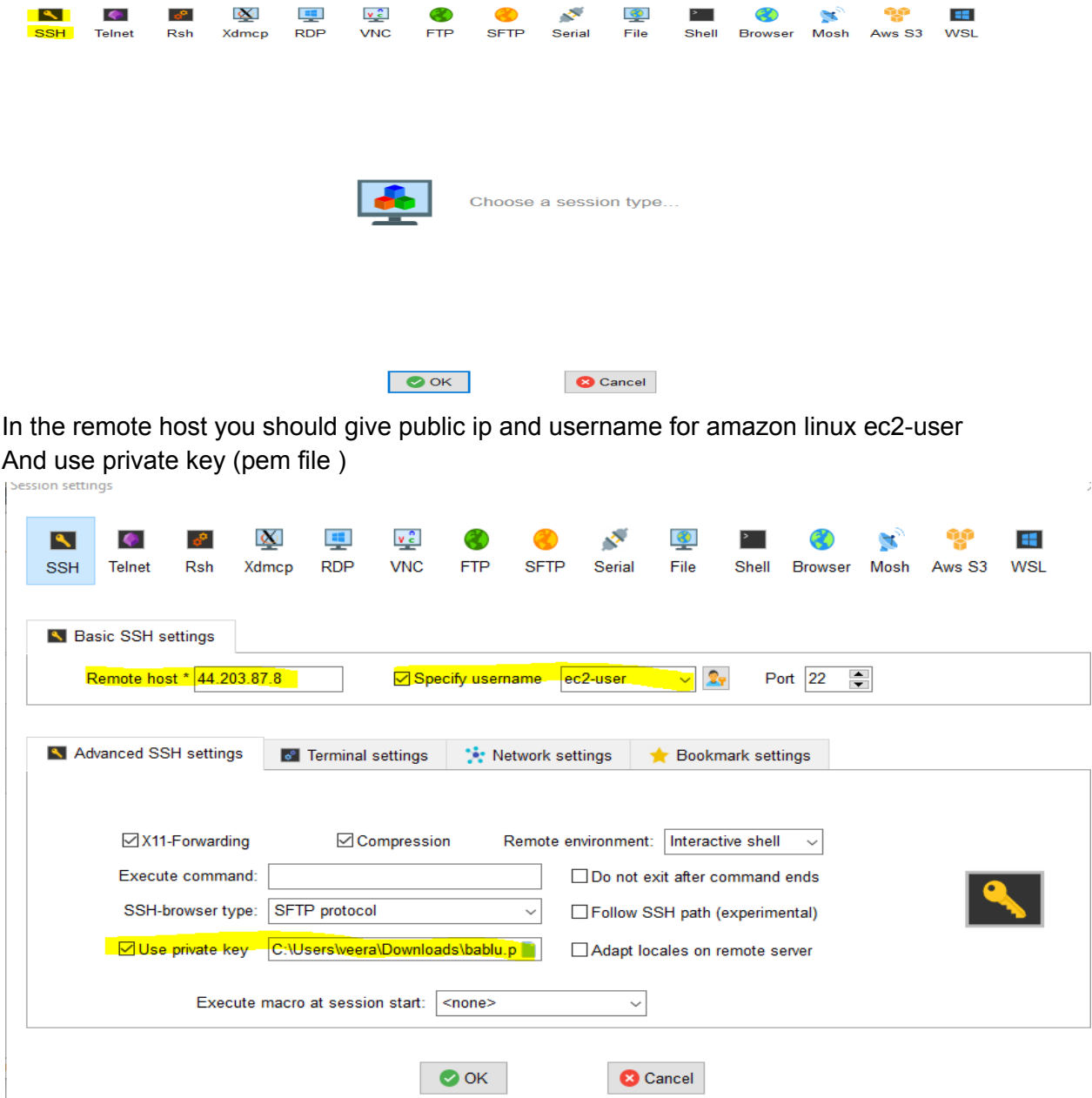
Copy the publicip address of particular instances



Popular tools to connect ec2 :

1. MobaXterm
2. Putty
3. git bash

Open mobaxterm:
Click on the session
Then choose ssh



After this you can see the workspace to login into server you can perform tasks

```
2. 44.203.87.8 (ec2-user) x +
• MobaXterm Personal Edition v21.5 •
(SSH client, X server and network tools)

> SSH session to ec2-user@44.203.87.8
• Direct SSH : ✓
• SSH compression : ✓
• SSH-browser : ✓
• X11-forwarding : ✗ (disabled or not supported by server)
> For more info, ctrl+click on help or visit our website.

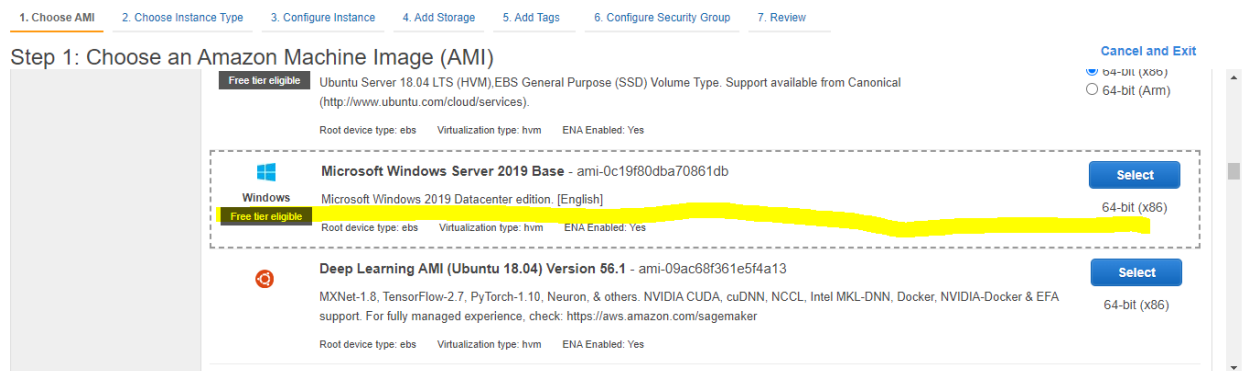
  _ | (-| - )
 _ | (-| - /
 _ | \ | _ |
Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
8 package(s) needed for security, out of 14 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-92-220 ~]$
```

WINDOWS:.....

How to login to windows virtual machine

Click on launch instances and in the choose AMI field click on windows



Step 2:

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 families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Low to Moderate	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Step 3:

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. 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 instances1Launch into Auto Scaling Group

Purchasing option☐ Request Spot Instances

Networkvpc-2f0c7152 (default)Create new VPC

SubnetNo preference (default subnet in any Availability Zone)Create new subnet

Auto-assign Public IPUse subnet setting (Enable)

Hostname typeUse subnet setting (IP name)

DNS Hostname☒ Enable IP name IPv4 (A record) DNS requests☒ Enable resource-based IPv4 (A record) DNS requests☐ Enable resource-based IPv6 (AAAA record) DNS requests

Placement group☐ Add instance to placement group

Cancel Previous Review and Launch Next: Add Storage

Step4:

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

Step 4: Add Storage

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.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0ce4ad4a65b3d72e7	30	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypte

Add New Volume

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.

Shared file systems

Step5:

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 ⁱ	Protocol ⁱ	Port Range ⁱ	Source ⁱ	Description ⁱ	
RDP ^v	TCP	3389	Custom ^v 0.0.0.0/0	e.g. SSH for Admin Desktop	
<button>Add Rule</button>					



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:

[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

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.



Improve your instances' security. Your security group, launch-wizard-25, 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-0c19f80dba70861db



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 (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

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

Step8:

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. Amazon EC2 supports ED25519 and RSA key pair types.

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](#).

Select a key pair

☒ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

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


Here select on particular server and click on the connect and the rdp client click on generate password it may takes 4 minor time and aks for

EC2 > Instances > i-06da20e03284ffc7 > Get Windows password


Get Windows password [Info](#)

Retrieve and decrypt the initial Windows administrator password for this instance.

To decrypt the password, you will need your key pair for this instance.

 **Key pair associated with this instance**
bablu


Browse to your key pair:

 Browse


Or copy and paste the contents of the key pair below:


And then click on browse select the pem file from local and then decrypt it

To decrypt the password, you will need your key pair for this instance.

 **Key pair associated with this instance**
bablu

Browse to your key pair:

 Browse

 **bablu.pem**
1.704KB

Or copy and paste the contents of the key pair below:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAizeksy6ADgt7VGftWqjoOC+dNS6BKmq4L+K/vd87O3uzekJk
Dy+S6hemcRpxYV56Hprs5GKjiXdatxbedly7pqfHyp9tnnRhu4a/QRdrM5i45f+b
UrO+oL+jC9qSATptXKH6ECoMAdmoYmgTJo8A4cceb5YZgfW0ilNAJgF9Fu+skvs
emiCkYm45r2PNdh/+VSISDAI+idRNWN7HI2L4D4U1SpCb1PODct0Xm3zZu86eEQu
bARigsAH/JNn83cpP5iTCv/7BffYnnrAh7WNMxvBxDv+B/bHPu1H1FABNllmxRN+
7FrwnX9qqw2O+ydF/3Vo25+AClcA86XxiJOdXQIDAQABAolBACXnMWVDbMPmJl7V
qM69G/RokklXdj1NiiYncxLL20GxRUbFGp7z0ekAJWW30FS1N0Rr48FOhb3gjAc7
-----
```

[Cancel](#) [Decrypt password](#)

And then download the remote desktop file and copy the password

Session Manager

RDP client

EC2 Serial Console

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:

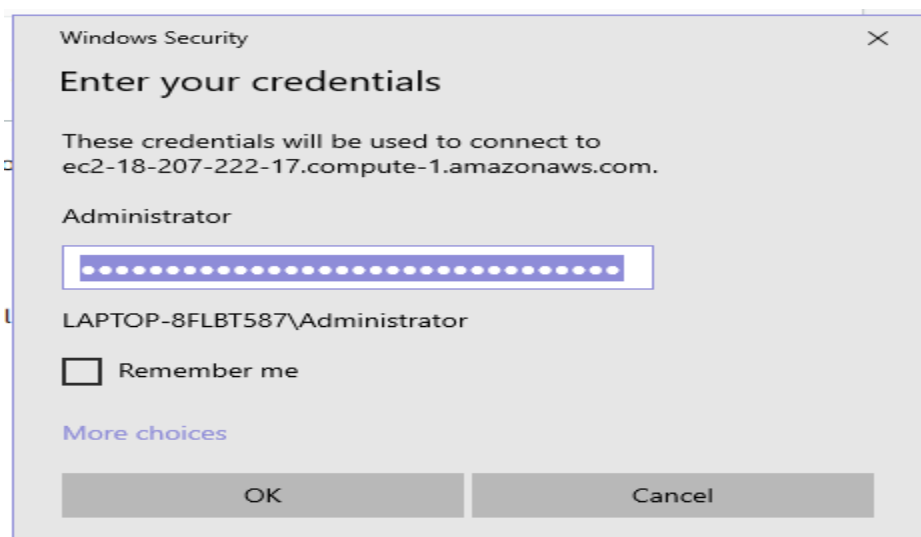
Download remote desktop file

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

Public DNS	User name
ec2-18-207-222-17.compute-1.amazonaws.com	Administrator
Password	
zu8bl&vfY%UMqD\$el6qDgo.LN;nlznFL	

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

then open the downloaded remote desktop file and copy the password in to it



Then you will see the new windows server launched

