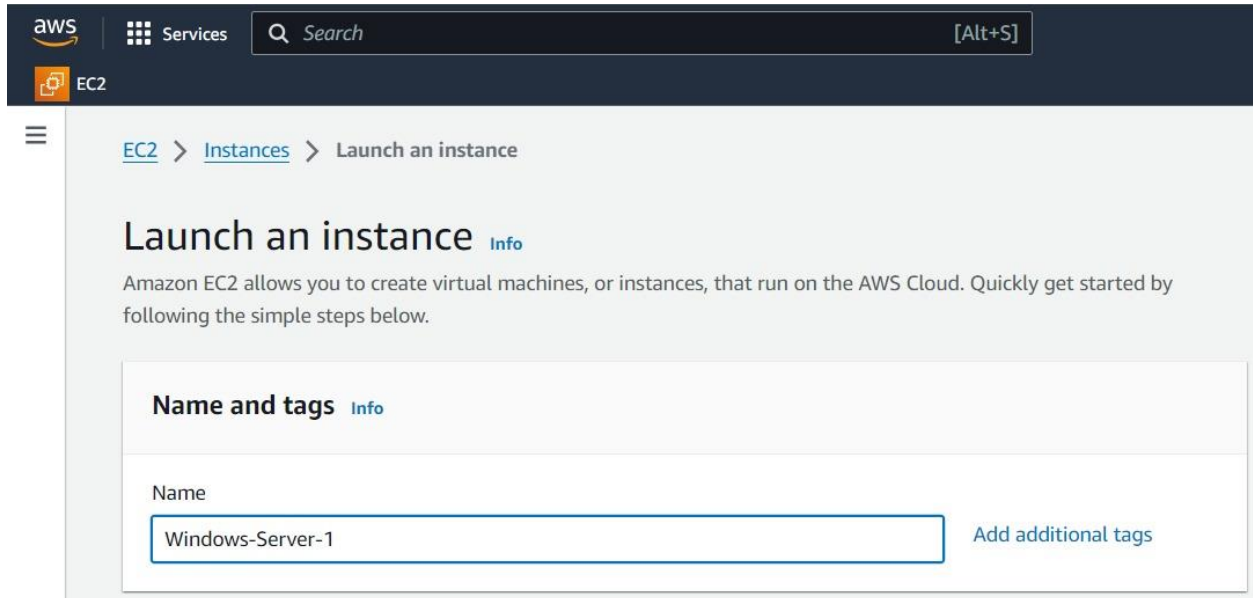


# TASK 1

Aim: (A)Deploy a **Windows Instance** In **Another Windows Instance**

Steps:

1) Create an windows instance on EC2 (**Windows-Server-1**)



aws Services Search [Alt+S]

EC2

EC2 > Instances > Launch an instance

## Launch an instance [Info](#)

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.

### Name and tags [Info](#)

Name

Windows-Server-1 [Add additional tags](#)

## 2) Select Amazon Machine Image (AMI) as Windows and Select Windows Server Base 2016 or Later

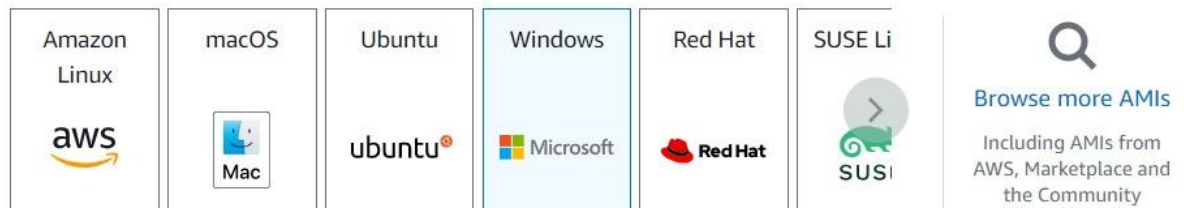
### ▼ Application and OS Images (Amazon Machine Image) [Info](#)

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**



#### Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base

Free tier eligible ▼

ami-09f6da726716a4ca6 (64-bit (x86))

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

#### Description

Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

## 3) Choose Instance Type As Per Your Requirements

### ▼ 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: 0.0724 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](#)

#### 4) Create a Key Pair and Select It

##### ▼ 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*

WindowsKey ▼

 [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.

#### 5) Edit Network Settings And Select Subnet : ap-south-1a OR ap-south-1b

##### ▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0cfb0aac3a4e1dd73  
172.31.0.0/16

(default) ▼



Subnet [Info](#)

subnet-08bc5ebefc896b5de

VPC: vpc-0cfb0aac3a4e1dd73 Owner: 851725375246

Availability Zone: ap-south-1a IP addresses available: 4089 CIDR: 172.31.32.0/20



 [Create new subnet](#) 

Auto-assign public IP [Info](#)

Enable ▼

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

6) In Inbound Security Group Rules, Set Type To “**rdp**” and Source Type as “**Anywhere**”

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 - optional	
Anywhere ▼		Add CIDR, prefix list or security		e.g. SSH for admin desktop	
		0.0.0.0/0 ✕			

⚠


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.


✕

Add security group rule

► Advanced network configuration

- 7) Get password from the created .pem key and use it to connect the rdp file and launch the Windows Instance

 Services  [Alt+S]

 EC2


Connect to your instance i-0b3665b87d43804c1 (Windows-Server) using any of these options

Session Manager

**RDP client**


EC2 serial console

Instance ID


 i-0b3665b87d43804c1 (Windows-Server)

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




ec2-43-205-98-61.ap-south-1.compute.amazonaws.com

Username [Info](#)

 Administrator ▼

Password

 P-fP(pUQ(\$jqK6FXSk.(Qp8\*AakG5=\*P

8) Now Create Another Windows Instance Using The Above Steps (**Windows-Server-2**)

aws Services Search [Alt+S]

EC2

EC2 > Instances > Launch an instance

## Launch an instance [Info](#)

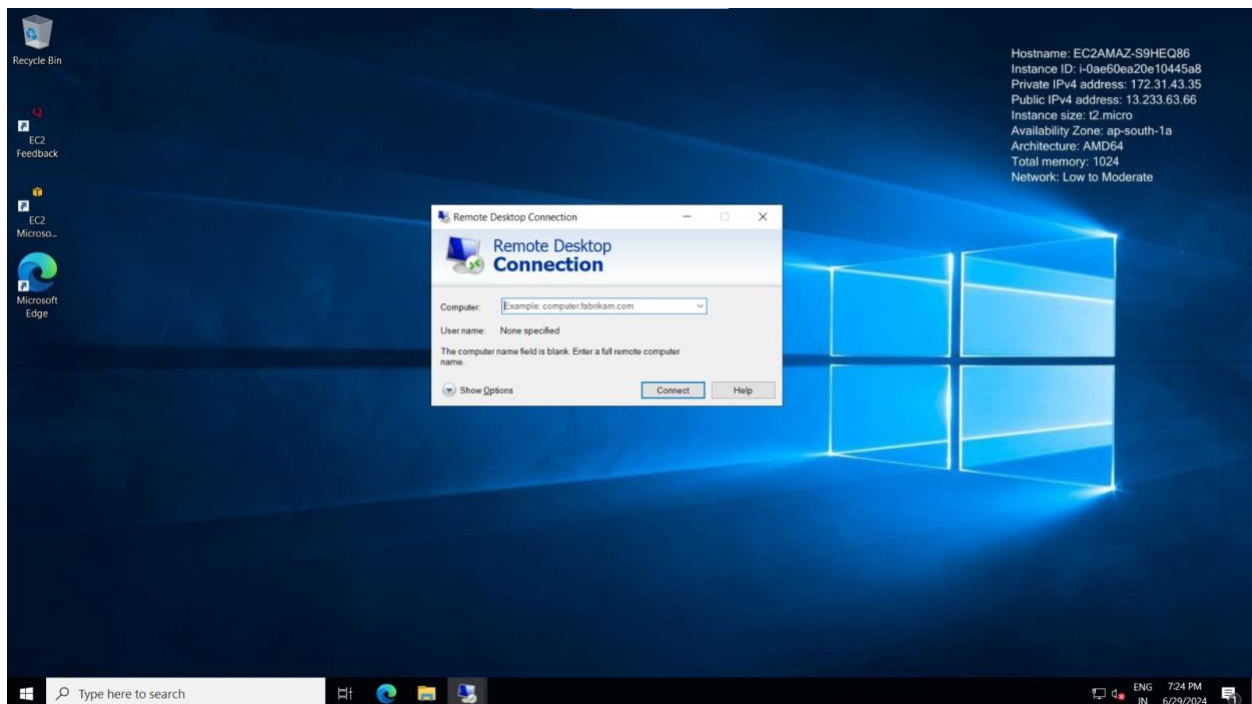
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

### Name and tags [Info](#)

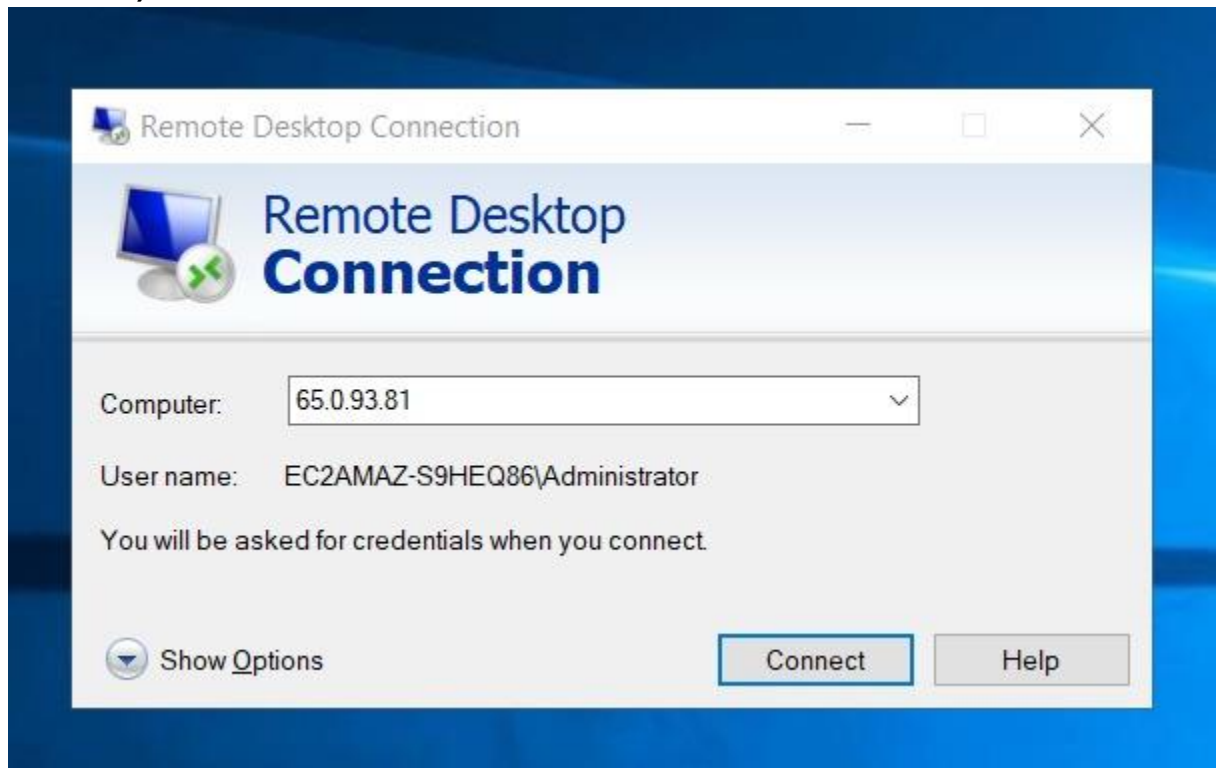
Name

Windows-Server-2 [Add additional tags](#)

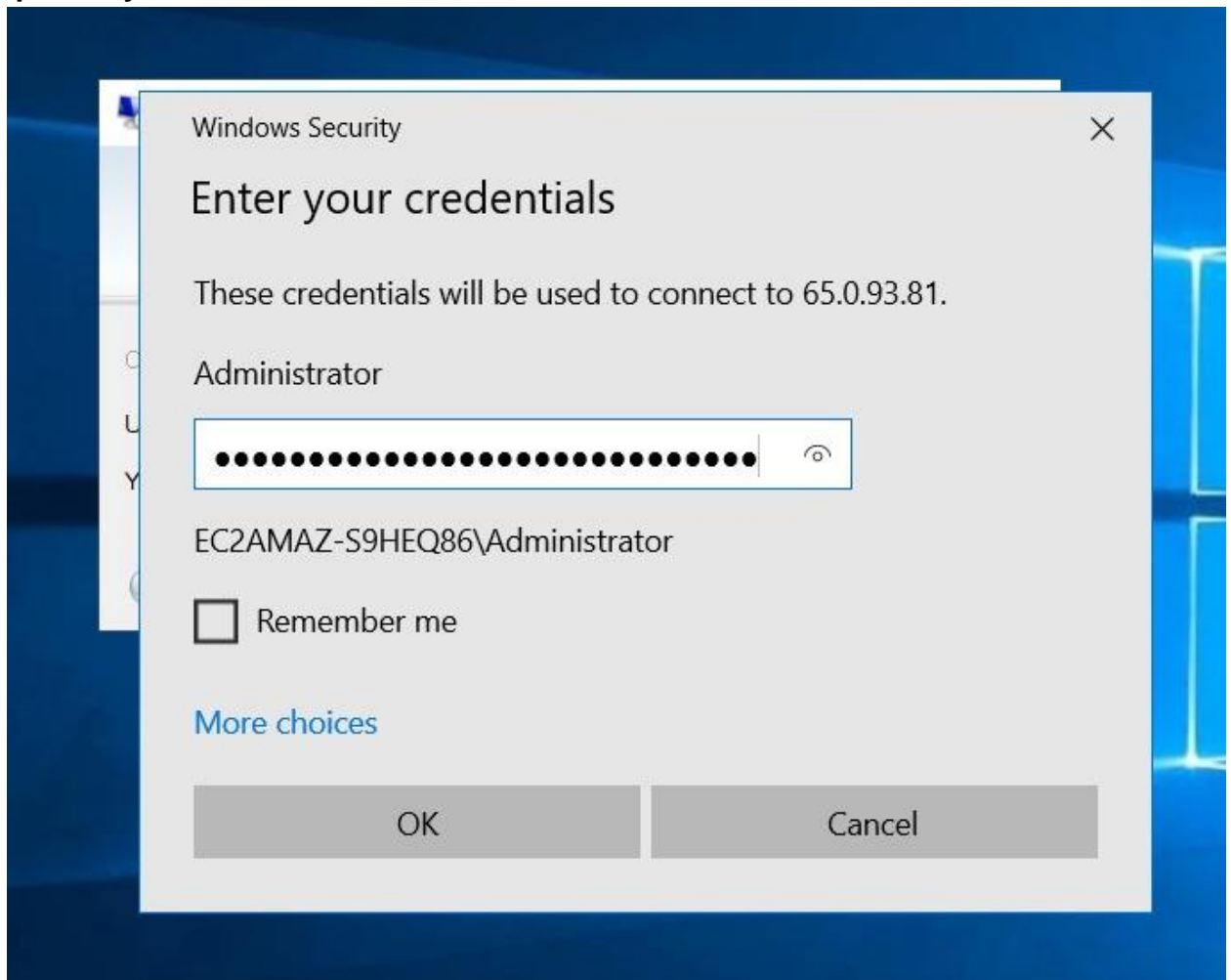
9) Now once the first instance(**Windows-Server-1**) is launched then type “**Remote Desktop Connection**” in Windows Search Bar



- 10) Now enter the Public IPv4 OR Public DNS of the Second Instance (**Windows-Server-2**) and click on **Connect**

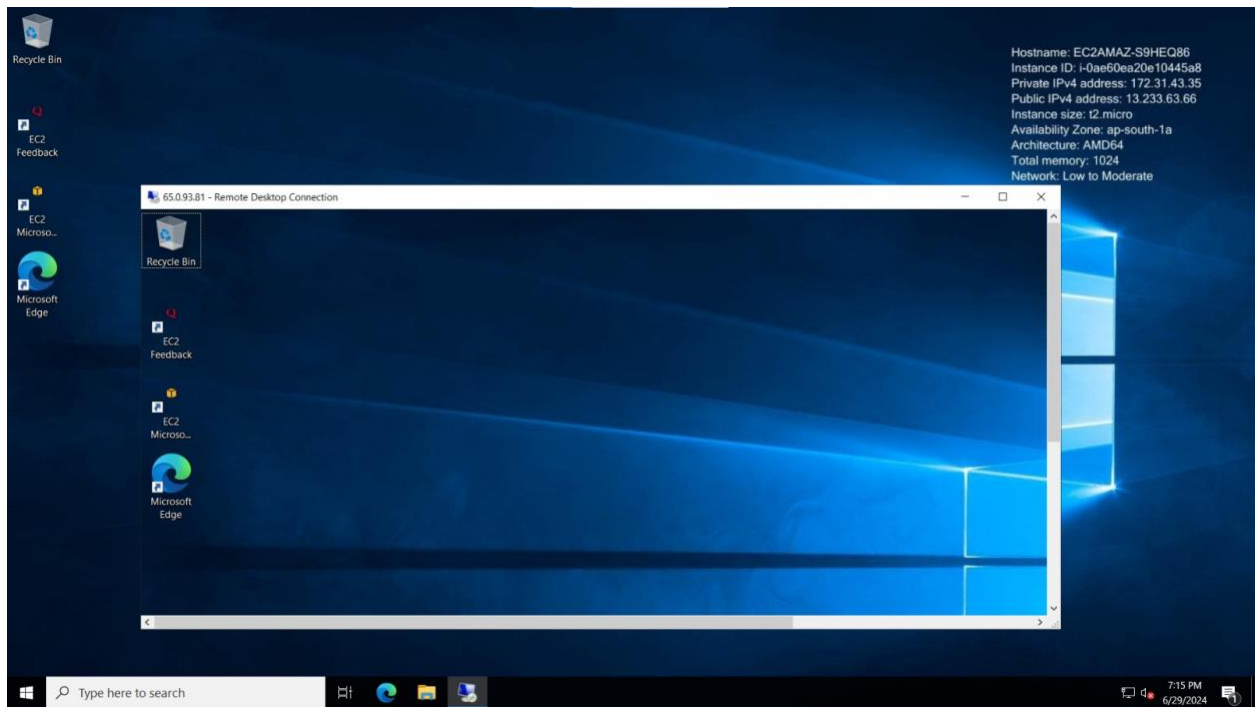


- 11) Now Enter Username as “**Administrator**” and Password as your **decrypted .pem key** and click OK





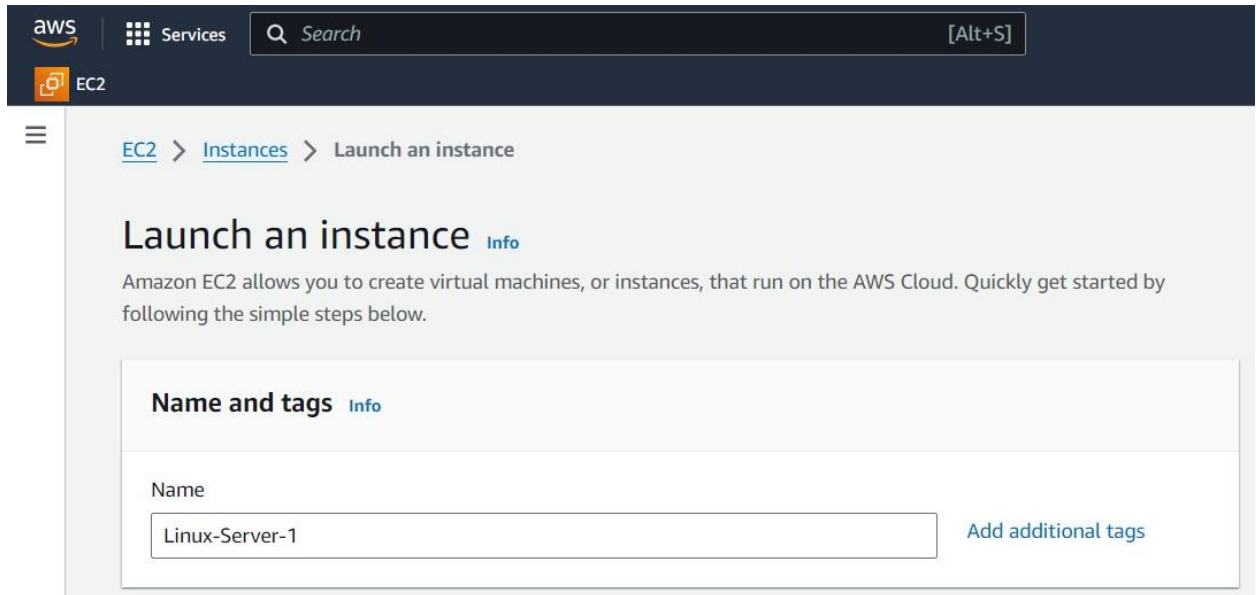
## 12) And Here is Your **Windows Instance** Inside **Another Windows Instance**



Aim: (B) Deploy a **Linux Instance** In **Another Linux Instance**

Steps:

- 1) Create an linux instance on EC2 (**Linux-Server-1**)



The screenshot shows the AWS Management Console interface for launching an EC2 instance. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and an '[Alt+S]' shortcut. Below the navigation bar, the breadcrumb trail reads 'EC2 > Instances > Launch an instance'. The main heading is 'Launch an instance' with an 'Info' link. A descriptive paragraph 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.' The 'Name and tags' section is highlighted, featuring a 'Name' label and a text input field containing 'Linux-Server-1'. To the right of the input field is a link to 'Add additional tags'.

aws | Services | Search [Alt+S]

EC2

EC2 > Instances > Launch an instance

## Launch an instance [Info](#)

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.

### Name and tags [Info](#)

Name

Linux-Server-1 [Add additional tags](#)

## 2) Select Amazon Machine Image (AMI) as Amazon Linux and Select Amazon Linux Server 2023

**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**

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux

**Amazon Machine Image (AMI)**

**Amazon Linux 2023 AMI** Free tier eligible

ami-04f8d7ed2f1a54b14 (64-bit (x86), uefi-preferred) / ami-0150a7de9db550188 (64-bit (Arm), uefi)  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**

Amazon Linux 2023 AMI 2023.5.20240624.0 x86\_64 HVM kernel-6.1

## 3) Create a Key Pair and Select It

**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*

LinuxKey2 ▼ [Create new key pair](#)

- 4) In Inbound Security Group Rules, Set Type To “**ssh**” and Source Type as “**Anywhere**” and Add New Security Group Set Type To “**http**” and Source Type as “**Anywhere**”

The screenshot shows the AWS Management Console interface for configuring Inbound Security Group Rules. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and the 'EC2' icon. The left sidebar shows a hamburger menu. The main content area is titled 'Inbound Security Group Rules' and contains two rule configurations.

**Security group rule 1 (TCP, 22, 0.0.0.0/0)** [Remove]

Type	Protocol	Port range	Source type	Source	Description - optional
ssh	TCP	22	Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

**Security group rule 2 (TCP, 80, 0.0.0.0/0)** [Remove]

Type	Protocol	Port range	Source type	Source	Description - optional
HTTP	TCP	80	Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

- 5) Now Launch This Instance (**Linux-Server-1**) and Create Another Linux Instance In EC2 (**Linux-Server-02**) following the above steps

The screenshot shows the AWS Management Console 'Launch an instance' page. The top navigation bar is identical to the previous screenshot. The left sidebar shows a hamburger menu. The main content area has a breadcrumb trail: 'EC2 > Instances > Launch an instance'. Below the breadcrumb is the title 'Launch an instance' with an 'Info' link. A descriptive paragraph follows: '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.' Below this is a section titled 'Name and tags' with an 'Info' link. It contains a 'Name' label and a text input field with the value 'Linux-Server-02'. To the right of the input field is a link 'Add additional tags'.

EC2 > Instances > Launch an instance

## Launch an instance

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.

**Name and tags**

Name

Linux-Server-02

Add additional tags





- 8) Now in this instance create a file using **touch** named as .pem key of your second instance and edit it file by using **vi** and paste the encrypted file contents in that file and close it and make sure to type command after editing the file [**>chmod 400 "filename"**] to ensure key is not publicly viewed

```
root@ip-172-31-47-231:/home/ec2-user
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAoZFR0KA93MRemT6LqT8HEr0h37NAI1s+MTd9YCMcnzonv27l
DpcLRqTgd+9YauXvShuI5ryJ9m6ni812wKf7BIZ1H5GiNLY5FQHJvoXGthfx1jV7
66wPENXWw4e8fhg8qDhPsMk+AdaKEfmrVbFfOjQzFPN/yp0GVm00JxDZLbU4luJz
p7DDjUlKJ1KmdkjagB8A0UNz7qyfBxFdAn8xc2yW0X/69eV+bsowWcVsgdzR/TF+
JqZ4gsYa5GNxHE/T4UURZzWTmXI16GyCSmM5LoSg7fqGjwShmcNrw3n9I1tyiADH
fPoofq9rGqJMcev8qbLw5+4VvXaRC9mU30hiCwIDAQABAoIBAFr9yZLYPATSPuiV
NfiK04SNKb+fZvbCk0MKmjyHBD6CdRI19SCDZmFRx+0jyaridiJJYY95DUXRSeDN
RRz5PcBtrRarYSvImFtBV4pKMwAoehWgP5SxoQZ9N+eE0V4+biLbG95XZ+mHftlK
v/iR3Syda0tYW1cTmhcggh2ec8ILxjVDVm144UsTSq8pcX7tTeJ/0HZGwnWj9S/8y
ogmIddgiEtv6RgwHSC0q1ELeYUT5AMRh0cia6h47rnHjAz2DvlEvrX0vADaofv1u
SB1iAyNMpGFdNl/JSs/o+0wPUASU7nMxjPIb555LbWoElzmSP2IHTbJ2vlj7T7IV
EG2jAdECgYEA8UQvOFzBGRNJaW3Hkj1QSHR42ndaL+WC/14cADm5apXq9uu6W7Ag
b102b40h7FeLdPbKl9hbD9+i5anmHeP27NoXd9JXaGw7+kMsm7zS/hYW3sleypix
R/7rx317Jkwd1UcxgjGajrafYeduwg6+WH/eiI1K3X7lZ3vj7dijnjDMCgYEAq28s
QY6gZQvhnA0HHTwfne5Kc9rtE0SD0bhvaAFqTXJlBLNT3zhc0Fr8zXgPwoiBqtZK
0aN/ip2XE166E5CirLe/TxG4uboo3N/GBI9y+KWHY5d6Vt0ISqnRj0txKhZnJYyb
I49o09PKgv/nHkg6jm5aN+owPkmciiLbuqmpeskCgYB5T/iSVYk+i4UZPvrfWnQ0
ymPOLb8qYDP7JZ3cuymxH0qy95qP6cKVXIA3mC9+ABL+L+10ZnR7Sc7FviUYGH0b
YRn1xMzWk60g1dADSvGokwDS6tv/8MELW3HAsCaQ/iruB8ssFLcLVWZUuyLk7rb1
Fv6VGL5xGxJMc24LNUUpQIwKBgGww7S0yZedfaDKdx1ieW03CxRn4wEQ48zgXvbdV
rVDTMQ2WXwgw+YJXadQCQW/z1mGKe62Eka1Za06+KZDPZtq52/J6rKoJ4mACmWwn
Ylepn5gqsPrA48q7AZR9wh1dlfQPGJmImA+XSecCuUlTLCfXY3iGQ4wLyM8k0Kct
C9iBAoGATLPaY6LgSVg886PBMAUqm/g0e4xZcG9s3uV0Wnga/TbxMbtGKx3Q6lZN
qh6xbz3iDp8PviYmaUpXd3Q06qPa7w9ECpKNYKNuEVwVgTWhp/dYg85TYBdPxSMZ
a+dBHv4KDvT3DooDhY2Qb3l8NtaYfT6MfmMTVlI0tnhS3QmesHo=
-----END RSA PRIVATE KEY-----
```

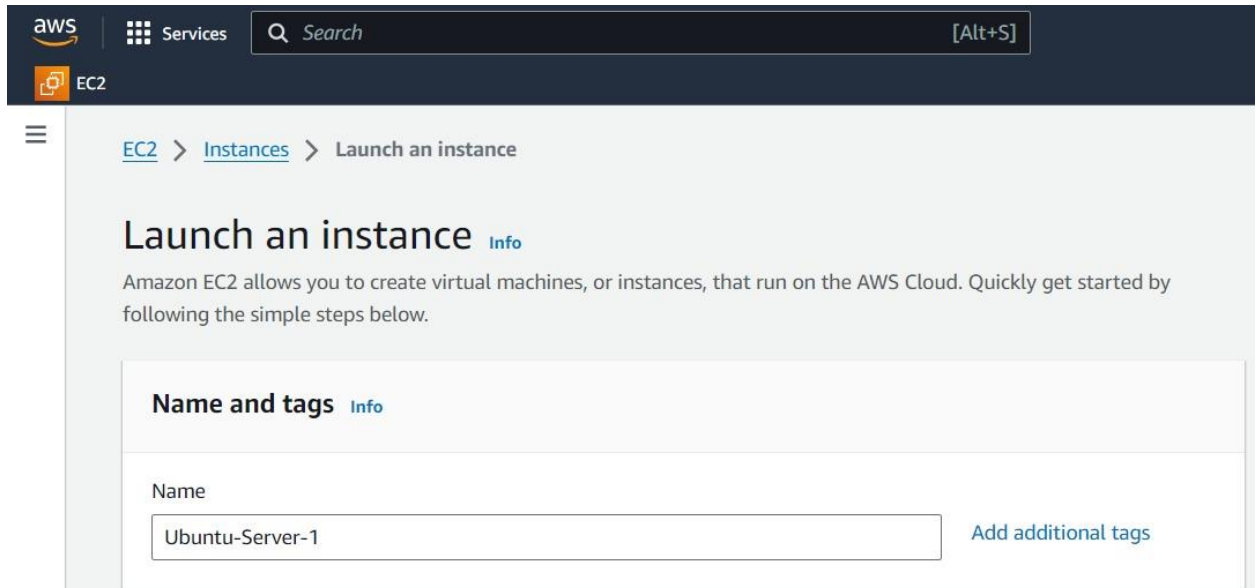
- 9) Now Run Your Second Linux Instance by Deploying it on Your **First Linux Instance** by inserting the ssh client of the Public DNS with .pem key file location on your instance computer and that's your Linux Instance Inside Another Linux Instance

[illegible]

Aim: (C) Deploy a **Ubuntu Instance** In **Another Ubuntu Instance**

Steps:

- 1) Create an ubuntu instance on EC2 (**Ubuntu-Server-1**)



The screenshot shows the AWS Management Console interface for launching an EC2 instance. The top navigation bar includes the AWS logo, 'Services', a search bar, and an '[Alt+S]' shortcut. The left sidebar shows the 'EC2' icon. The main content area has a breadcrumb trail: 'EC2 > Instances > Launch an instance'. The title 'Launch an instance' is followed by an 'Info' link. Below the title, a paragraph 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.' A section titled 'Name and tags' with an 'Info' link contains a 'Name' label and a text input field with the value 'Ubuntu-Server-1'. To the right of the input field is a link that says 'Add additional tags'.

aws | Services | Search [Alt+S]

EC2

EC2 > Instances > Launch an instance

## Launch an instance [Info](#)

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.


### Name and tags [Info](#)


Name


Ubuntu-Server-1 [Add additional tags](#)



## 2) Select Amazon Machine Image (AMI) as Ubuntu and Select Ubuntu Server 24.04 LTS

 Services  [Alt+S]


 EC2





▼ 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


[Quick Start](#)


 Amazon Linux


 macOS

 Ubuntu

 Windows

 Red Hat

 SUSE Li

 [Browse more AMIs](#)  
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type  
ami-0f58b397bc5c1f2e8 (64-bit (x86)) / ami-0dda4ba9a42839a4b (64-bit (Arm))  
Virtualization: hvm   ENA enabled: true   Root device type: ebs

Free tier eligible ▼

Description

Canonical, Ubuntu, 24.04 LTS, amd64 noble image build on 2024-04-23


## 3) Create a Key Pair and Select It

▼ 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*

▼

 [Create new key pair](#)

- 4) In Inbound Security Group Rules, Set Type To “**ssh**” and Source Type as “**Anywhere**” and Add New Security Group Set Type To “**http**” and Source Type as “**Anywhere**”

The screenshot shows the AWS Management Console interface for configuring Inbound Security Group Rules. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and the 'EC2' service icon. The left sidebar shows a hamburger menu. The main content area is titled 'Inbound Security Group Rules' and displays two rules. Rule 1 is for SSH (Type: ssh, Protocol: TCP, Port range: 22, Source type: Anywhere, Source: 0.0.0.0/0, Description: e.g. SSH for admin desktop). Rule 2 is for HTTP (Type: HTTP, Protocol: TCP, Port range: 80, Source type: Anywhere, Source: 0.0.0.0/0, Description: e.g. SSH for admin desktop). Each rule has a 'Remove' button.

Type	Protocol	Port range	Source type	Source	Description - optional
ssh	TCP	22	Anywhere	0.0.0.0/0	e.g. SSH for admin desktop
HTTP	TCP	80	Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

- 5) Now Launch This Instance (**Ubuntu-Server-1**) and Create Another Instance In EC2 (**Ubuntu-Server-2**) following the above steps

The screenshot shows the AWS Management Console interface for launching an EC2 instance. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and the 'EC2' service icon. The left sidebar shows a hamburger menu. The main content area is titled 'Launch an instance' and includes a breadcrumb trail: 'EC2 > Instances > Launch an instance'. Below the title is a brief description of Amazon EC2. The 'Name and tags' section is visible, with a text input field for the instance name containing 'Ubuntu-Server-2' and a link to 'Add additional tags'.

Launch an instance

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.

Name and tags

Name

Ubuntu-Server-2

Add additional tags

6) Type **Command Prompt** and **Run as Administrator** on Your Local Computer

```
Administrator: Command Prompt

Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>
```

7) Now Run Your Linux Instance by Deploying it on Your **Command Prompt** by inserting the ssh client of the Public DNS with .pem key file location on your local computer

```
Select ubuntu@ip-172-31-45-126: ~
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh -i "C:\Users\ITSKDM\Downloads\UbuntuKey.pem" ubuntu@ec2-13-126-43-39.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-126-43-39.ap-south-1.compute.amazonaws.com (13.126.43.39)' can't be established.
ED25519 key fingerprint is SHA256:6BMRbT4sRzkHMjbn0KnN33s66VnAejQpf6Y1ZIZMrQQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-126-43-39.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1008-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sun Jun 30 20:13:32 UTC 2024

System load:  0.07               Processes:    108
Usage of /:   23.2% of 6.71GB    Users logged in: 0
Memory usage: 20%               IPv4 address for enX0: 172.31.34.227
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-34-227:~$ sudo su
```



- 8) Now in this instance create a file using **touch** named as .pem key of your second instance and edit it file by using **vi** and paste the encrypted file contents in that file and close it and make sure to type command after editing the file [**>chmod 400 "filename"**] to ensure key is not publicly viewed

```
ubuntu@ip-172-31-34-227:~$ sudo su
root@ip-172-31-34-227:/home/ubuntu# touch UbuntuKey.pem
root@ip-172-31-34-227:/home/ubuntu# vi UbuntuKey.pem
root@ip-172-31-34-227:/home/ubuntu# root@ip-172-31-34-227:/home/ubuntu# chmod 400 "UbuntuKey.pem"
root@ip-172-31-34-227:/home/ubuntu# pwd
```

```
C:\ root@ip-172-31-34-227: /home/ubuntu
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEAhRVRoAMpzTbdg6UICr5bqeqmSR0vpDjpXa4QMM610aEKewqi
9rUoFDiQJFifLVuE79PcPL7+qoukOVxfzhmBHcTNJnz moyJZ0YLk52T5p4J0+ybP
EUXtgzHu2AzyKZhbDMCv4bzRZi8t8GRLY+36zZgvs g831qKH3mT0eh1L+0qzj+rt
OfHrYCCCCGQSjzuxWe9fFKW/yx2qg7uaYHefNdq+bYaZoJ9KyvWb6EYAb/R3cQjdq
W00r7PZL4VqstL0b/raEHCWVWNAgU8AxG9fjzIPB3qbdSdeInj9nZTPHg7TW8xS4
hLhXf9UCLWAV7zYFXac9gWniLZ0vEytbjZJ2QwIDAQABAoIBA F8EPJX5DDR XUsp1
3osFJB7pyLVuF74xX/ShnS+rtkaoKvp0QvX5XiiiF+Q4n0Y1Y4BfkHkv6B20Nc3
a70TpArkAvDSxjx8/xHF2baX8mM1kl3qdHbJrW05DmU0wQUPoRo2zJxoGj1RvAPh
J65+L83wNUV09hIJUuZmpMCtABwENQIVpSFKM20k4+Y/ULKa5MvvnWJAc1h0g6aY
OAQTFXxikMg5CNXHdRV20FYyzfokj/jPV9As7HLhCv/l3JXIWir16hvBM02cCb35
gUwstPvYl/ThtNFq9cjgh0yd/EuLoueJsJAzRxW0sasfaoPKX35PcT2XHFya0zBA
hpxSRxkCgYEAzWfZzFV7ACd1Sv7Jg/eeBU0C3b5KbLhp80ztn7no6FDNYWafPVFR
ZcXYdKhWd8PeAJOVmybQ4Viup/65m05T601X6h4a/s5SJeDFpuhyvHOMstozQwHD
JxMW16qe73wVXp95b3uZDWBb4S2nsTHi6czm/bf61110TC2zd9iv980CgYEApd0T
b6Zat4UcKfXFJonEBs51/0SZDIEQvpZQc08eBddHkqs7gmeMfs88K00NHgiID2NJ
jRKSrvxfgYV5Dg2yq9UwSbi8Xe7fwxTGeDPVMj41Qt fGrvvRkmVxtadqGpPqCgcK
TLJJAsjtK9hX23ZMh6IRRhFKLff93vAmSGG+9k8CgYAsW7YMS5WBhgPtizJnnmzw
xh3NV0/pRLYUxdM3QEXNDc4cr7XJ3yrN6LkDEGuD97eUtkqDtBE96RHm07qvKG3N
DenjdFbuGg5hgbYNgntsusN0aGzTlqjXYmb3cjBalZhj09q8uZtm6R10draVLKnN
RePIfRfdtJe5GdF9Gz19LQJ/G9wGZ7qJgknZcTLW6qI5Suti5n2fN3uN1HVRdFM8
F78RRpF8bWr3LlWgxT1zdpf4Qp1qvUdhSkU5xYelzbZ/TF2Cvt9IxH5bF21l7MrI
BKhuScv0k2+4w95G0zzjLZNCvGxyTm+j09PsAnFUUIiOUjnmrN46l34QJmIwC/hf
GwKBgQCnbDNHi00gCJWniYmnaIKdm4d3XP+nWwIZg5QzgAkRsxT5s/Vo1wUuD0it
w+Pg dViTz6UJ252hw1II5TC30bSyHydyWSKnNgxu1pGeg8JrwgbxwHBnQVEQog8S
tep4sQCknGUFrXtmwWljQqNrngjvpFTsqBfrm+qsgAfH9246dw==
-----END RSA PRIVATE KEY-----
```

- 9) Now Run Your Second Ubuntu Instance by Deploying it on Your **First Ubuntu Instance** by inserting the ssh client of the Public DNS with .pem key file location on your instance computer and that's your Ubuntu Instance Inside Another Ubuntu Instanc

```
❏ Select ubuntu@ip-172-31-45-126: ~
/home/ubuntu
root@ip-172-31-34-227:/home/ubuntu# ssh -i "/home/ubuntu/UbuntuKey.pem" ubuntu@ec2-13-127-35-53.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-127-35-53.ap-south-1.compute.amazonaws.com (172.31.45.126)' can't be established.
ED25519 key fingerprint is SHA256:9gyujDEQvcICFKx7ZQRW/cWsUguMctqZ0G9cA8yw1oI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-127-35-53.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1008-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Sun Jun 30 20:18:29 UTC 2024

System load:  0.0               Processes:           104
Usage of /:   23.2% of 6.71GB   Users logged in:    0
Memory usage: 19%              IPv4 address for enX0: 172.31.45.126
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-45-126:~$
```

Aim: (D) Deploy a **Linux Instance** In **Windows Instance**

Steps:

- 1) Create an windows instance on EC2 (**Windows-Server**)

aws Services Search [Alt+S]

EC2

EC2 > Instances > Launch an instance

## Launch an instance [Info](#)

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.

### Name and tags [Info](#)

Name

[Add additional tags](#)

## 2) Select Amazon Machine Image (AMI) as Windows and Select Windows Server Base 2016 or Later

### ▼ 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**



#### Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base

Free tier eligible ▼

ami-09f6da726716a4ca6 (64-bit (x86))

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

#### Description

Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

## 3) Choose Instance Type As Per Your Requirements

### ▼ 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: 0.0724 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](#)



#### 4) Create a Key Pair and Select It

##### ▼ 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*

WindowsKey ▼

 [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.

#### 5) Edit Network Settings And Select Subnet : ap-south-1a OR ap-south-1b

##### ▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0cfb0aac3a4e1dd73  
172.31.0.0/16

(default) ▼



Subnet [Info](#)

subnet-08bc5ebefc896b5de

VPC: vpc-0cfb0aac3a4e1dd73 Owner: 851725375246

Availability Zone: ap-south-1a IP addresses available: 4089 CIDR: 172.31.32.0/20



 [Create new subnet](#) 

Auto-assign public IP [Info](#)

Enable ▼

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



6) In Inbound Security Group Rules, Set Type To “**rdp**” and Source Type as “**Anywhere**”

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 - optional		Info
Anywhere ▼		Add CIDR, prefix list or security		e.g. SSH for admin desktop		
		0.0.0.0/0 ✕				

⚠


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.


✕

Add security group rule

► Advanced network configuration

- 7) Get password from the created .pem key and use it to connect the rdp file and launch the Windows Instance

 Services  [Alt+S]

 EC2


☰

Connect to your instance i-0b3665b87d43804c1 (Windows-Server) using any of these options

Session Manager


**RDP client**

EC2 serial console


Instance ID  
 i-0b3665b87d43804c1 (Windows-Server)

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**

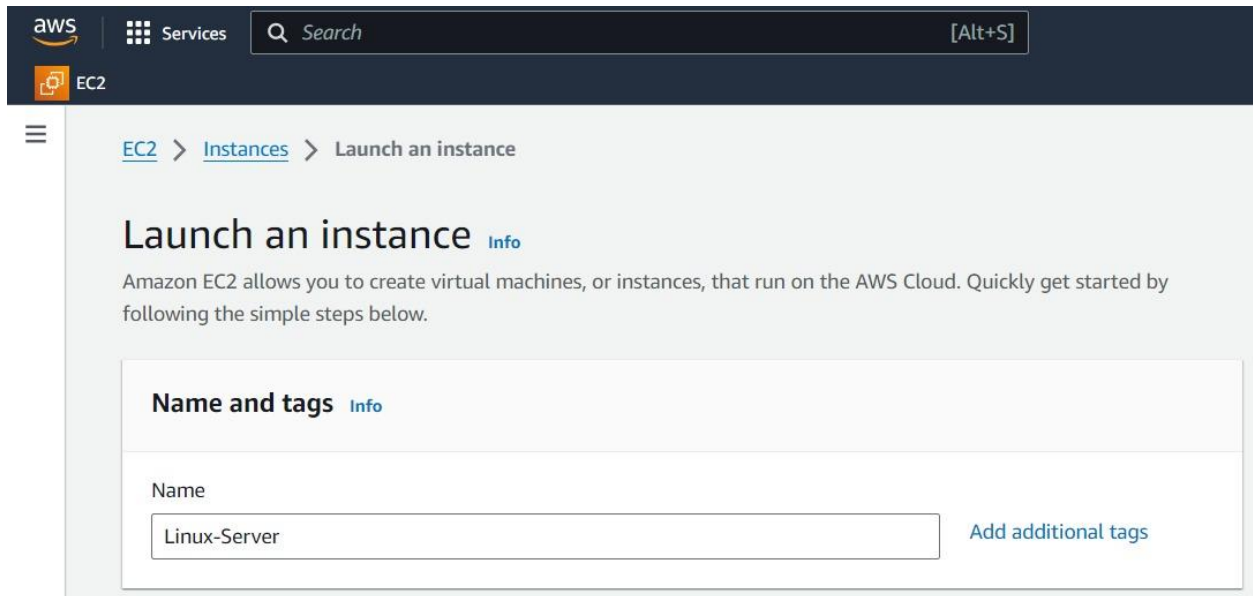
When prompted, connect to your instance using the following username and password:

Public DNS  
  
ec2-43-205-98-61.ap-south-1.compute.amazonaws.com

Username [Info](#)  
 Administrator ▼

Password  
 P-fP(pUQ(\$jqK6FXSk.(Qp8\*AakG5=\*P

## 8) Now create a linux instance (**Linux-Server**)



The screenshot shows the AWS Management Console interface for launching an EC2 instance. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar with the placeholder 'Search', and a keyboard shortcut '[Alt+S]'. Below this, the 'EC2' service is selected. The breadcrumb trail indicates the path: 'EC2 > Instances > Launch an instance'. The main heading is 'Launch an instance' with an 'Info' link. A descriptive paragraph 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.' The first step, 'Name and tags', is highlighted and also has an 'Info' link. It contains a 'Name' label, a text input field with the value 'Linux-Server', and a link 'Add additional tags'.

aws Services Search [Alt+S]

EC2

EC2 > Instances > Launch an instance

### Launch an instance [Info](#)

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.

#### Name and tags [Info](#)

Name

[Add additional tags](#)

9) Select Amazon Machine Image (AMI) as Amazon Linux and Select Amazon Linux Server 2023

**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

**Recents** | **Quick Start**

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

[Browse more AMIs](#)  
Including AMIs from AWS, Marketplace and the Community

**Amazon Machine Image (AMI)**

**Amazon Linux 2023 AMI**  
ami-04f8d7ed2f1a54b14 (64-bit (x86), uefi-preferred) / ami-0150a7de9db550188 (64-bit (Arm), uefi)  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Free tier eligible**

**Description**

Amazon Linux 2023 AMI 2023.5.20240624.0 x86\_64 HVM kernel-6.1

10) Create a Key Pair and Select It

**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*

[Create new key pair](#)

- 11) In Inbound Security Group Rules, Set Type To “ssh” and Source Type as “Anywhere” and Add New Security Group Set Type To “http” and Source Type as “Anywhere” and Launch the instance.

aws

Services

Search

[Alt+S]

EC2

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type

Info

ssh

Protocol

Info

TCP

Port range

Info

22

Source type

Info

Anywhere

Source

Info

Q Add CIDR, prefix list or security

0.0.0.0/0 X

Description - optional

Info

e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)

Remove

Type

Info

HTTP

Protocol

Info

TCP

Port range

Info

80

Source type

Info

Anywhere

Source

Info

Q Add CIDR, prefix list or security

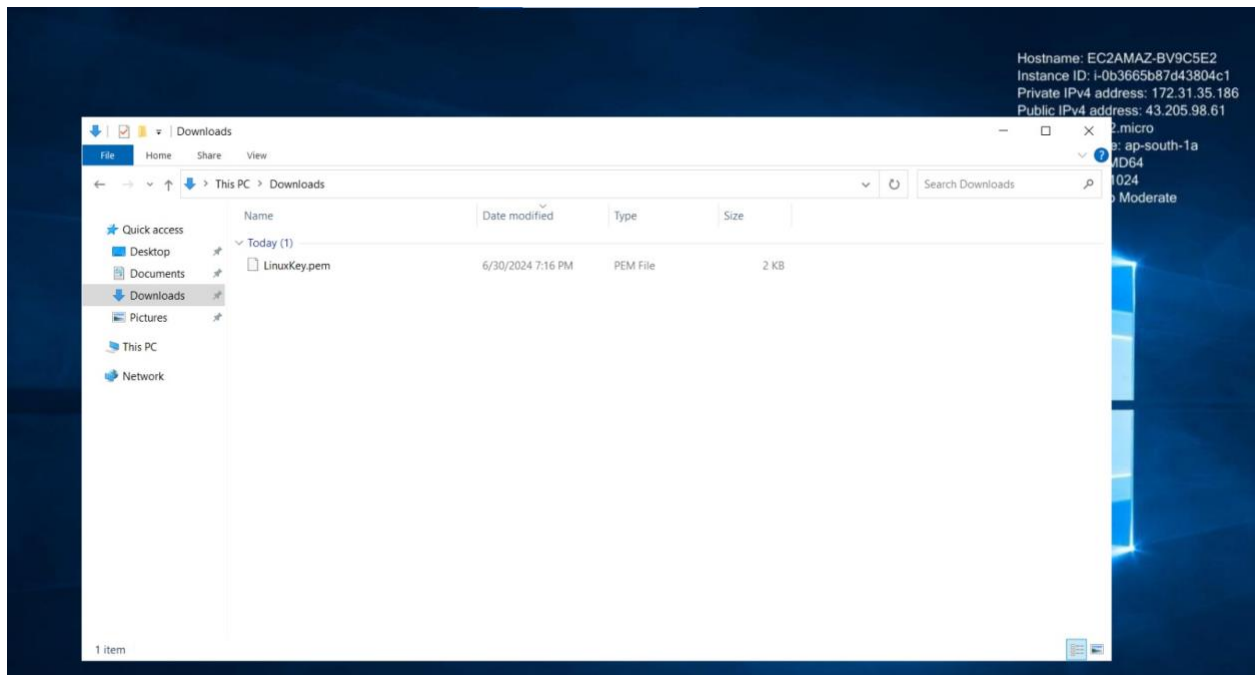
0.0.0.0/0 X

Description - optional

Info

e.g. SSH for admin desktop

12) Now Open The Windows Instance and Paste the .pem key of The Linux Instance



13) Now open command prompt in the Windows Instance and Change the directory where the .pem key is saved and Now Run Your **Linux Instance** by Deploying it on Your **Windows Instance** by inserting the ssh client of the Public DNS with .pem key file location on your instance computer and that's your Linux Instance Inside a Windows Instance.

