Contents

[Creating Free Instance Account with AWS console 2](#_Toc90990898)

[Creating EC2 instance 3](#_Toc90990899)

[Launching EC2 Instance 6](#_Toc90990900)

[Windows (Windows Server R2) 6](#_Toc90990901)

[RDP Permissions (Windows Server) 7](#_Toc90990902)

[Linux (Kali Linux) 10](#_Toc90990903)

# Creating Free Instance Account with AWS console

Go to https://aws.amazon.com/ and create free tier account with free tier support

A screenshot of a computer

Description automatically generated with medium confidence

# Creating EC2 instance

Under **Build a solution 🡪 Launch a virtual machine**

Graphical user interface, application

Description automatically generated

Now you can select various free tier instances that are free to use although it would have low operating capacity.

Go to **AWS Marketplace 🡪 Search for your instance**

In this example I will search for Microsoft Windows Server 2012 R2 Base version as that is eligible for Free Tier

Graphical user interface, text, application, email

Description automatically generated

Select the appropriate instance.

On the next page, go to Continue, where you will be able to choose which Tier you can choose (in our case we will choose Free tier as shown below)

Will select the t2.micro free tier and press 🡪 **Review and Launch**

A screenshot of a computer

Description automatically generated

In the next page, Press **Launch**

You will be asked to either create a key pair or Use existing 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.

Graphical user interface, text, application

Description automatically generated

Download the key pair, store it in a **secure location** on the computer (Probably under user where other users logged in cannot access). And then press **Launch Instance**

*Note: - It may take time for instances to launch, give some time to load.*

*Note: - If the instance does not show up, check for a different region for your instances to load up*

Graphical user interface, text, application

Description automatically generated

You can check your instances under 🡪 Services 🡪 EC2

It would look something like this, also to check the individual instances click on the **Instance ID**

Graphical user interface, text, application

Description automatically generated

# Launching EC2 Instance

## Windows (Windows Server R2)

Launching instance for windows Server would include connecting using RDP Session.

As shown in the previous Chapter, Windows server would use the password in the download Key pair plus the public key.

*Note: - This password is not the typing password, it is the key pair, once you decrypt that pair, you will receive an arbitrary password which you can then use to login to your windows machine*

Go to **Instaces** 🡪 Select the **Instance ID** 🡪 Press **Connect** 🡪 **RDP Client**

Click on the **Get password** Tab 🡪 Browse the password (key pair you saved earlier)

Graphical user interface, text, application

Description automatically generated

Decrypt the password to get a password for logging into the windows machine, copy that password and save it a safe place on the computer. Also note the username which is generally **Administrator.**

Next thing is to download the **Remote Desktop File** for the RDP session

Graphical user interface, text, application, email

Description automatically generated

Save the instance, and then open the RDP session to login

It will ask you for permissions as it is the first time you will be connecting to that instance.

## 

## RDP Permissions (Windows Server)

Press connect,

Graphical user interface, text, application, email

Description automatically generated

Input the password that you already saved on your computer,

And you will end up with this screen which says that is the certificate proper or not, here you can either directly just connect or view the certificate by clicking on the tab

Graphical user interface, text, application, email

Description automatically generated

After opening the certificate, go to **Details** tab and scroll down until you see **Thumbprint 🡪** Keep that value open.

Graphical user interface, application

Description automatically generated

Crosscheck this value with the value in session manager.

Go to **Instances** 🡪 Select your **Instance ID** 🡪 **Actions** 🡪 **Monitor and Troubleshoot** 🡪 **Get system log** and check the values against the one shown in on the RDP session, if it all good go ahead and trust this certificate

And Voila! you are inside the free cloud instance 🡪 **Cloud Magic**

## Linux (Kali Linux)

For Linux it does vary a bit, as you would initially login using the command prompt on your windows machine or linux machine.

For linux you will using command prompt to login using ssh,

Open command prompt, and cd to the folder where the key pair is stored (Secret RSA key)

And to connect to the instance you use the following command

**Ssh -i kali.pem kali@public IP**

Kali.pem – RSA Secret key

kali@<public IP> - username kali @ public IP

*Note: - Copy paste the public IP address from going into the instance settings*

It will ask you for confirmation, press **Yes**

And now you will be inside the terminal of Kali linux

Shape, rectangle

Description automatically generated

## GUI configuration in Kali Linux

We will use VNC to connect using SSH to the kali linux server

Do update using

* **Sudo apt update**

Install Tight VNC server using

* **Sudo apt install xfce4 xfce4-goodies tightvncserver**

Press Enter once prompted

Installing gnome core

* **Sudo apt-get install gnome-core kali-defaults kali-root-login desktop-base**

Once prompted you can choose between ligthdm or gdm3

Configuration tightvncserver for resolution

* **Tightvncserver -geometry 1024x768**

Will require password to access, set a password

Check if connection is done,

* **Netstat -tulpn (**Check the port at which it connects 5901**)**
* A picture containing graphical user interface

  Description automatically generated

Connect to VNC server

Go to command prompt from windows host machine,

Use the following command to create ssh tunnel to vnc server

* **Ssh -L 5901:localhost:5901 -N -f kali@public ip -I kali.pem, press it and it will start running**

To run it as GUI, download VNC viewer from the internet, install it and run it

Connect it using the **localhost:5901** in the field

Graphical user interface, text, application

Description automatically generated

Press enter and input the password and you are into the kali linux.

After running the commands, it will work as a gui (safe and secure)