

## WAZUH

Wazuh is an open-source security monitoring platform that provides threat detection, integrity monitoring, incident response, and compliance reporting. It's often used for security information and event management (SIEM), log analysis, and intrusion detection.

Summary: I am using window aws instance instead of my local workstation & ingesting logs to wazuh , so that I can see my logs in WAZUH & perform different operations like vulnerability detection , FIM etc .

Currently or by default only EventViewer logs are getting ingested in the wazuh .

Visit <https://wazuh.com/> & click on wazuh cloud

The Wazuh website homepage features a prominent banner titled "The Open Source Security Platform" with the subtitle "Unified XDR and SIEM protection for endpoints and cloud workloads." Below the banner are two buttons: "Install Wazuh" and "Free Cloud Trial". To the right, a preview of the Wazuh dashboard is shown, displaying various security metrics and charts.

**Wazuh Dashboard Preview:**

- Alerts level evolution:** A line chart showing alerts over time.
- MTRE ATT&CK:** A donut chart showing the distribution of MITRE ATT&CK techniques.
- Top 5 agents:** A bar chart showing the top 5 agents by alert count.
- Security alerts table:** A table with columns: Time, Agent, Agent name, Technique ID, Tactic ID, Description, Level, and Rule ID. The first row shows an alert from agent 004 on a Windows system at 10:00:00, with a description of "Signed Script Proxy Execution C:\Windows..." and a level of 10.

### Create account & Deploy the environment.


### Create your environment


An environment contains all the Wazuh components ready for you to use. Once created, you only need to enroll your Wazuh agents to get started.


**Name**  **Region**


**What is your use case for the trial?**

### Select your profile

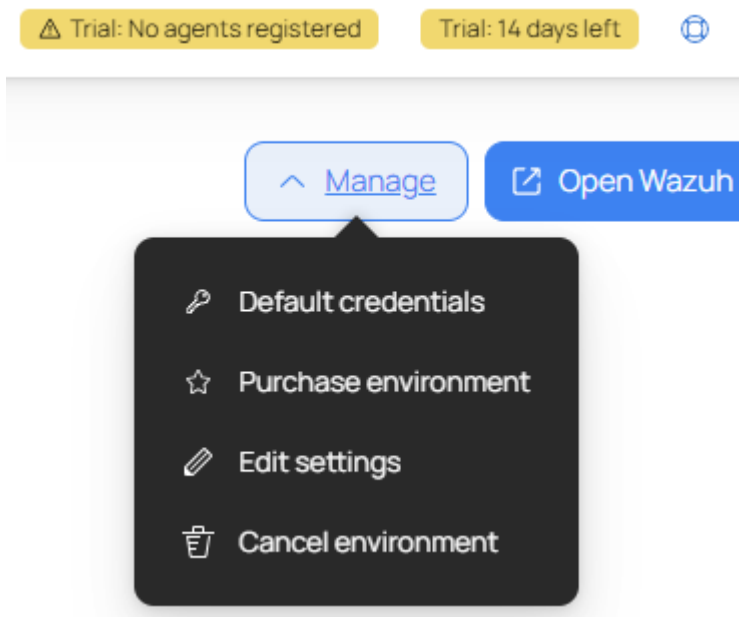
 **Small**

 **Medium**

 **Large**

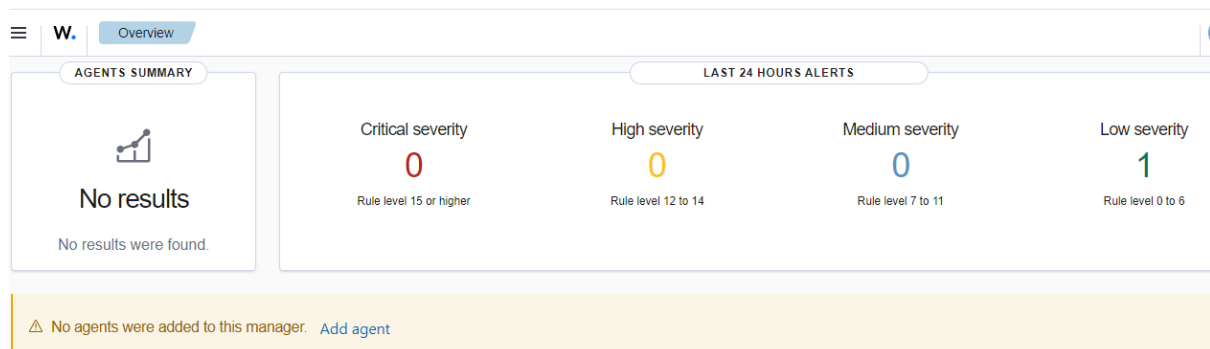
 **Custom**

Choose default credentials to login to Wazuh Cloud.

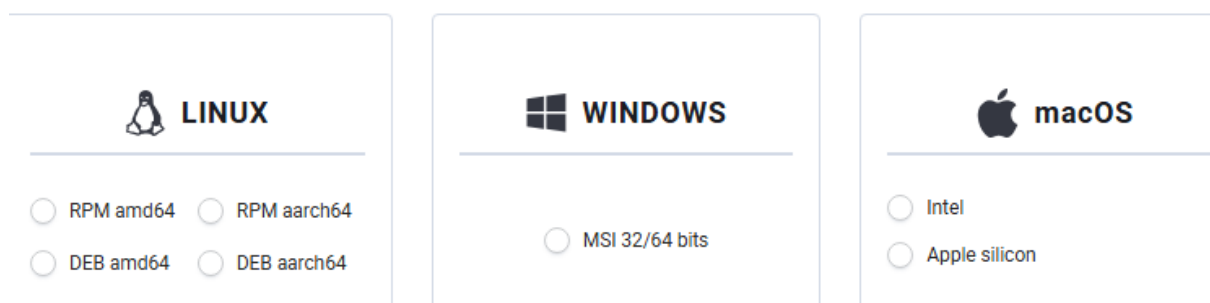


Wazuh Cloud use Elastic search in backend

Click on Add Agent



Select any end point , I am choosing windows



## Name any agent & keep it same in Select one or more existing groups:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ?

Agent name

① The agent name must be unique. It can't be changed once the agent has been enrolled. [↗](#)

Select one or more existing groups: ?

Default

## Paste the command in the endpoint to download the agent i.e powershell. For me its window

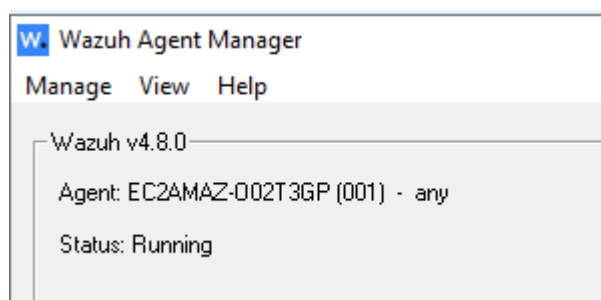
```
Invoke-WebRequest -Uri  
https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.0-1.msi -OutFile  
${env.tmp}\wazuh-agent; msixexec.exe /i ${env.tmp}\wazuh-agent /q  
WAZUH_MANAGER='xxxxxxx.cloud.wazuh.com'  
WAZUH_REGISTRATION_PASSWORD='xxxxxxxxxxxxxxxx'
```

## Start the service with below commands

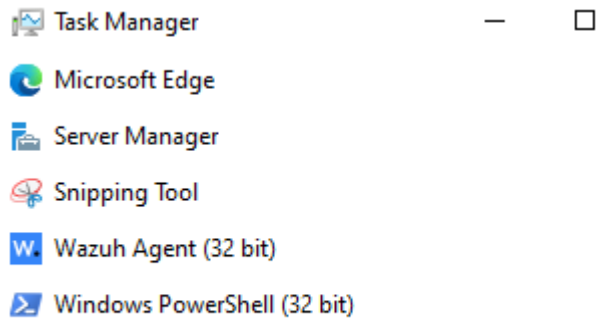
Start-Service -Name "wazuhSvc"

### To confirm that the service is running

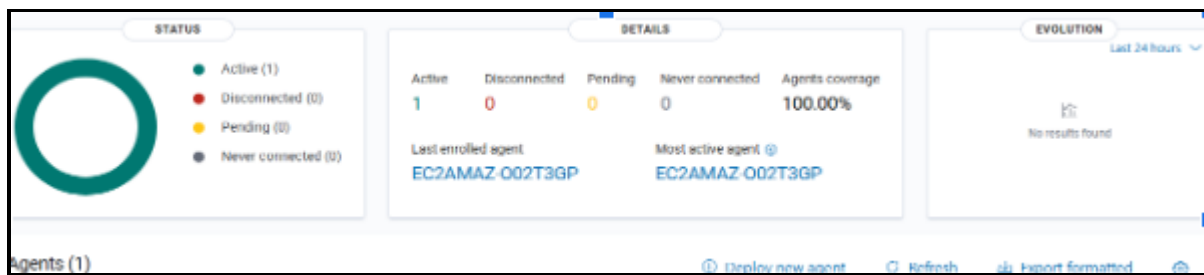
C folder- – ossec agent –win32ui.exe (double click ) –check the status



Check in the task manager for cross check



Now Check in Wazuh : check agent will be displayed



Note: We can add upto 100 agents means from 100 endpoints logs can be ingested in free wazuh cloud for 14th days without any credit card or providing any payment

## Sysmon Logs ingestion in wazuh:

### What is sysmon used for?

System Monitor (Sysmon) is one of the most commonly used add-ons for Windows logging. With Sysmon, you can detect malicious activity by tracking code behaviour and network traffic, as well as create detections based on the malicious activity.

**Sysmon** is part of the **Sysinternals software package**, now owned by Microsoft and enriches the standard Windows logs by producing some higher level monitoring of events such as process creations, network connections and changes to the file system.

Download Sysmon From :

<https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

Always run sysmon **with admin priv with xml data** so that sysmon knows what should be logged or what not .

The location of logs collected by Sysmon: Event Viewer -> Applications and Services Logs -> Microsoft -> Windows -> Sysmon folder.

So adding sys.xml file which have content which i have pasted from

<https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml>

Run with admin in cmd if not worked use ps with admin

```
PS C:\WINDOWS\system32> cd D:\Sysmon
PS D:\Sysmon> .\Sysmon64.exe -i .\sys.xml
```

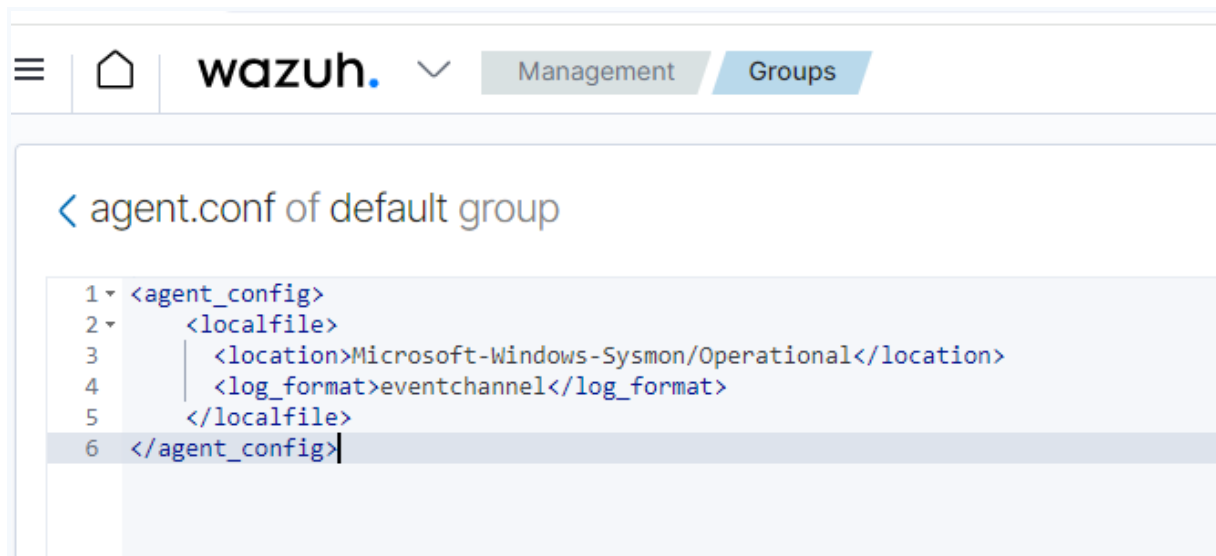
Reference : list-of-sysmon-event-ids-for-threat-hunting:

<https://systemweakness.com/list-of-sysmon-event-ids-for-threat-hunting-4250b47cd567>

Now we have to config the path sysmon in wazuh , so wazuh will know where the logs of sysmon is getting generated.

**Now configure wazuh:**

Enter the sysmon log path in Management –group – edit



```
<agent_config>
  <localfile>
    <location>Microsoft-Windows-Sysmon/Operational</location>
    <log_format>eventchannel</log_format>
  </localfile>
</agent_config>
```

Now check the logs in discover tab , you will able to see logs by name sysmon

**If you want to create max log in minimum time to confirm sysmon setup, you can use an automation tool which will do activity & create logs . Below tool is one of example.**

Before running the below tool to your env , disable your defender or other antivirus first. Try to run in sandbox environment only .

Download and **Run the bat file after extracting**

<https://github.com/NextronSystems/APTSimulator/releases/tag/v0.9.4>

**Window Defender Logs ingestion in wazuh:**

**Now configure wazuh:**

**Enter the sysmon log path in Management –group – edit**

```
<localfile>  
  <location>Microsoft-Windows-Windows Defender/Operational</location>  
  <log_format>eventchannel</log_format>  
</localfile>
```

**If you want to create max log in minimum time to confirm window defender setup, you can use an automation tool which will do activity & create logs . Below tool is one example.**

**Before running the below tool to your env , disable your defender or other antivirus first. Try to run in sandbox environment only .**

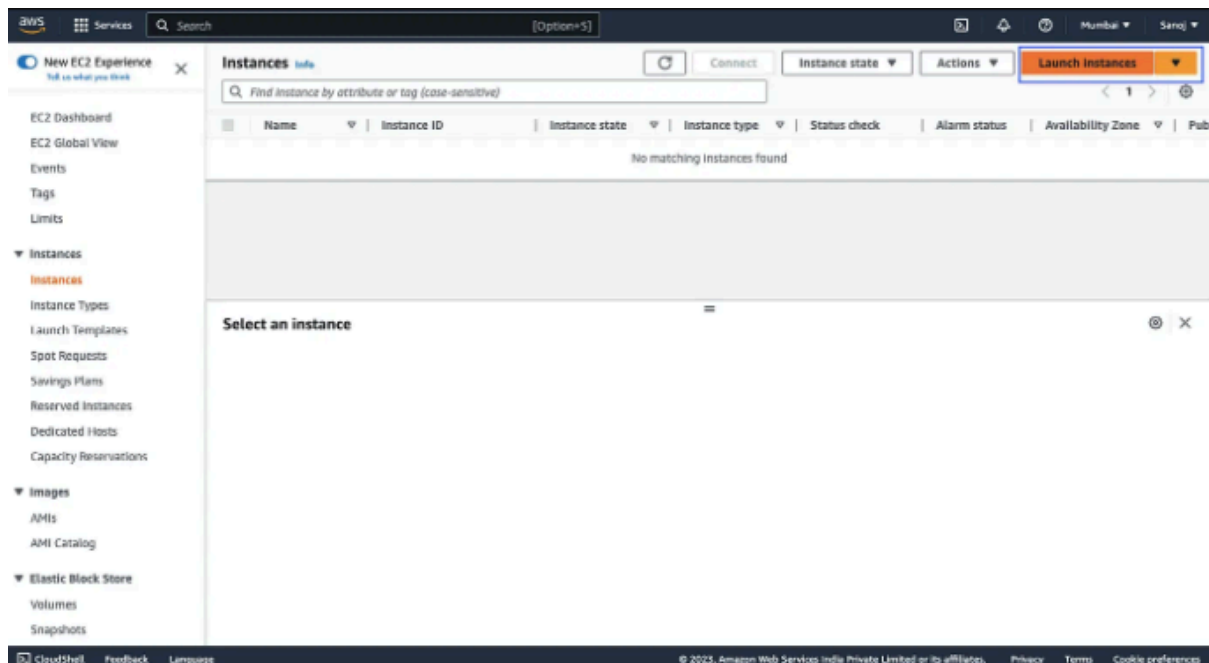
For testing defender log

<https://www.eicar.org/download-anti-malware-testfile/>

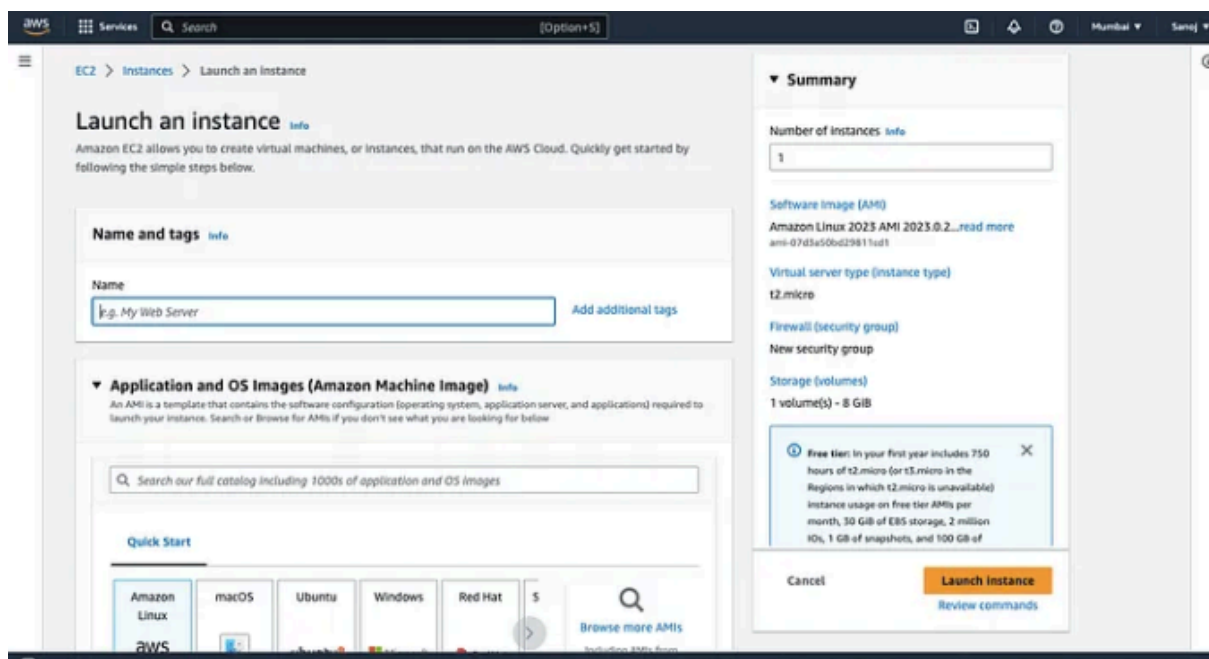
.\pse - i -s powershell

## **Set up AWS instances (I am using windows)**

**Step 1: Sign in to the AWS Management Console and click on the “Launch Instances “**

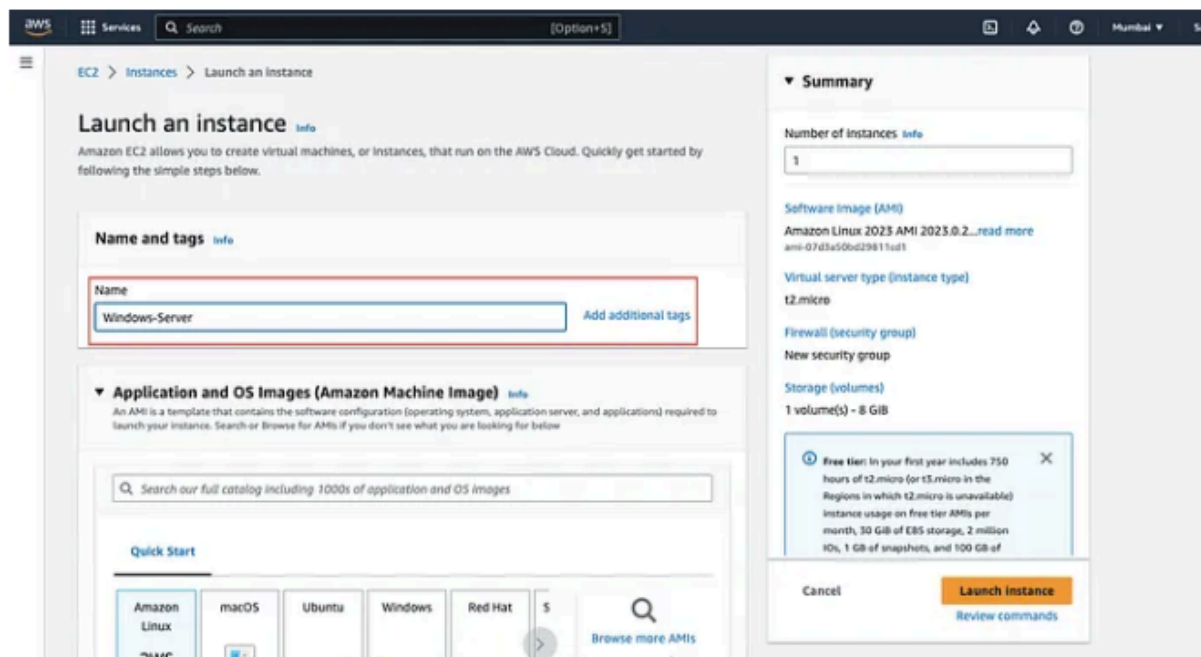


After clicking on the “Launch Instances” the following interface will appear.

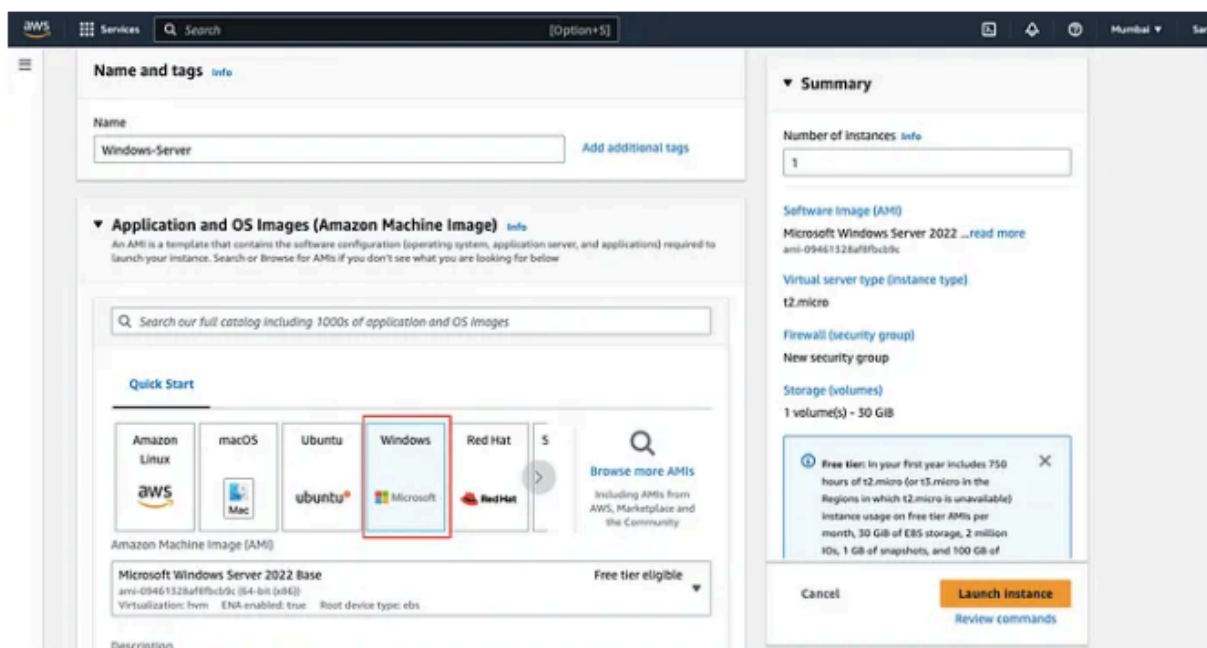


Step 2: Now give the Instance name, I gave the name “Windows-Server”. You can give any



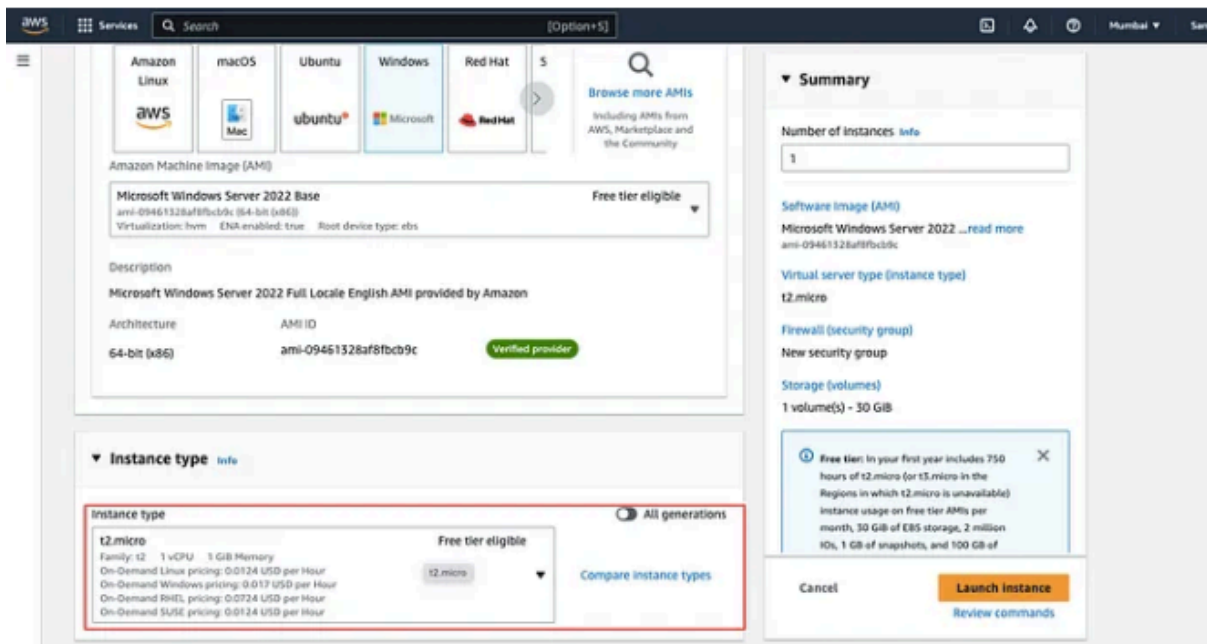


**Step 3: Select the AMI (Amazon Machine Image) or OS.**

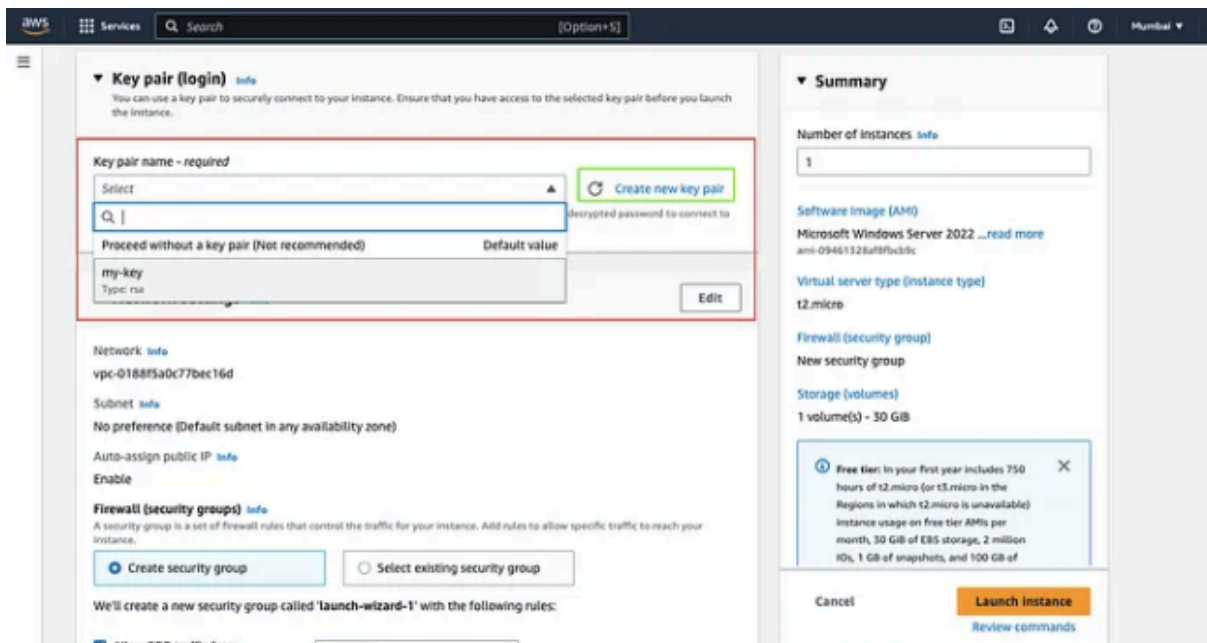


**Step 4: Select the Instance Type or Hardware Type, I selected t2.micro.**

**You can choose any one but for the above one you can choose the free one with less memory.**

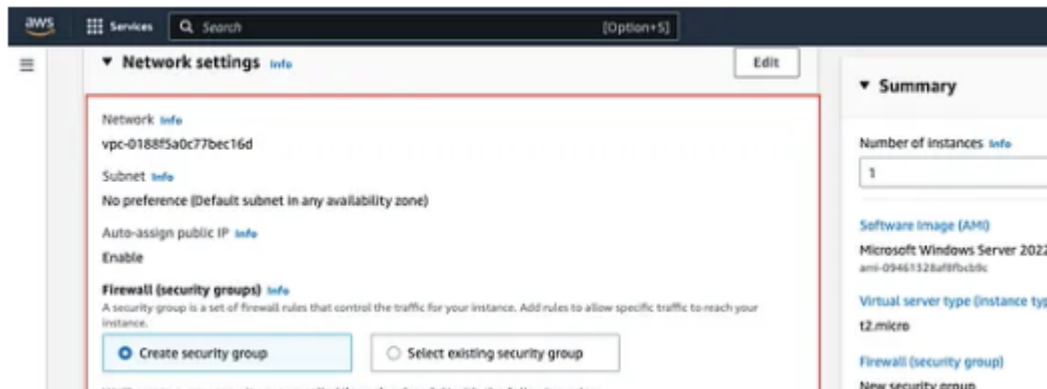


**Step 5: Select your “Key pair” by clicking on the Drop down menu, if you don’t have , create a new “key pair”.**

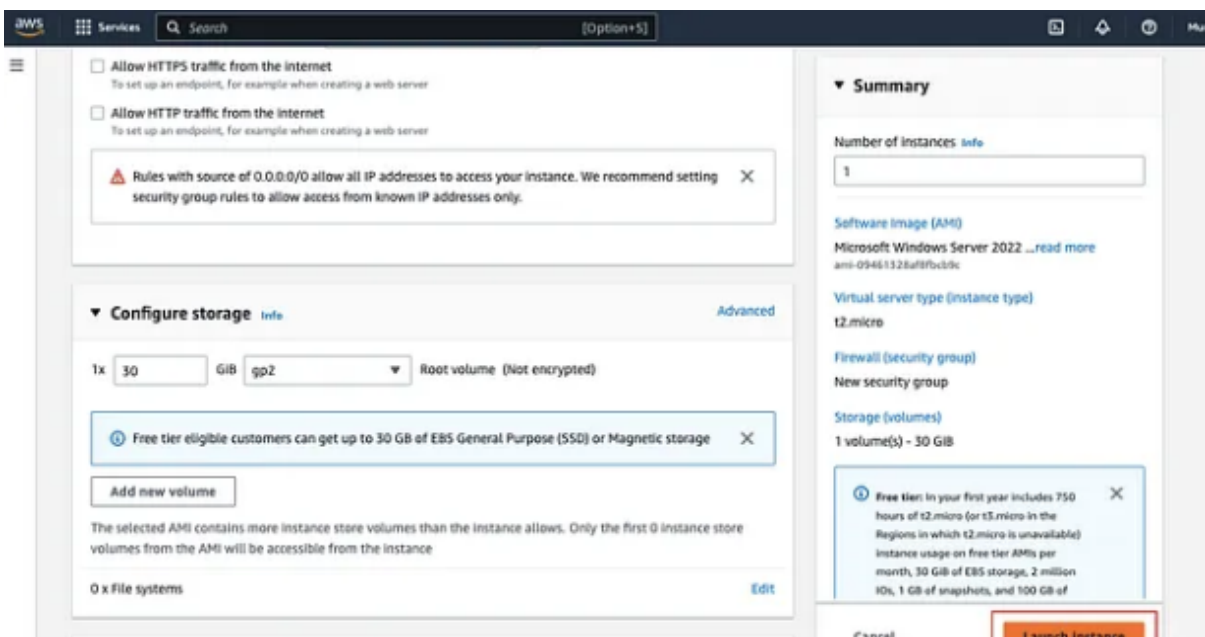


**Step 6: Select your security group if you have already if you don’t have a, create a new security group.**

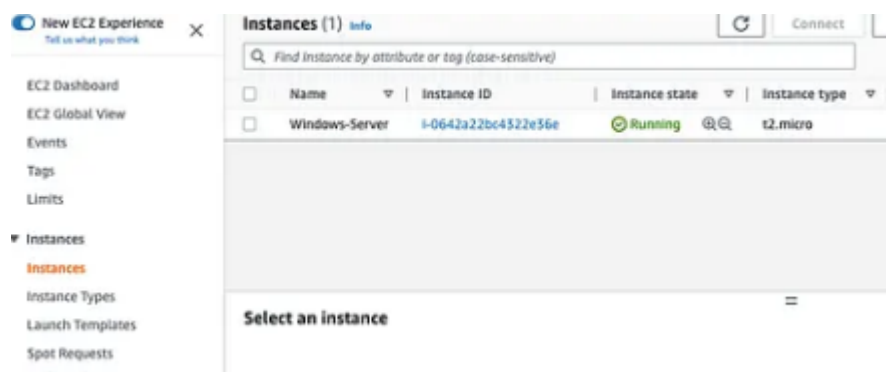
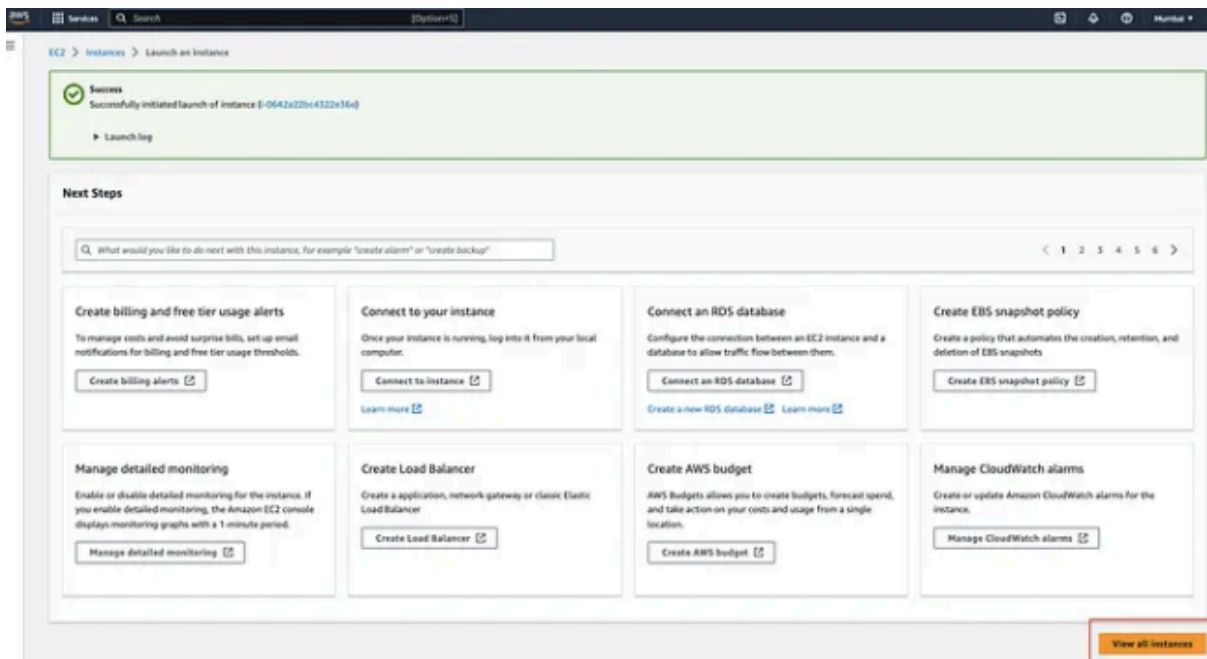
**Note: If you keep it as it is, AWS will create a new security group for you.**



**Step 7: Click on the “Launch Instance”.**

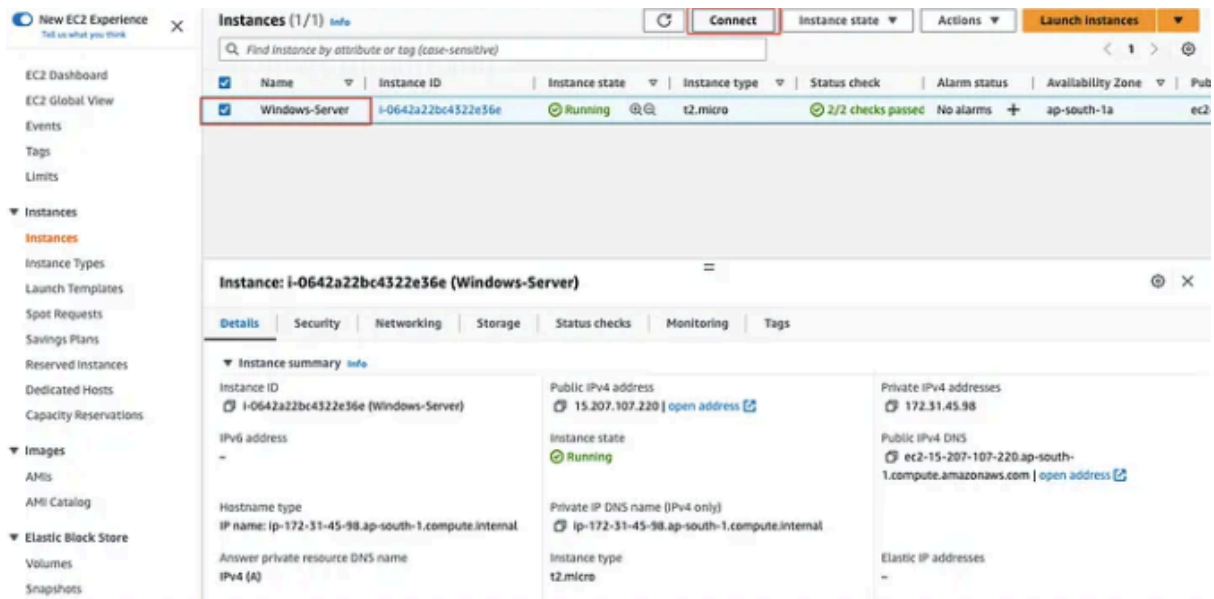


**After clicking on the “launch Instance” the following interface will appear, just click on the “View all instances”**



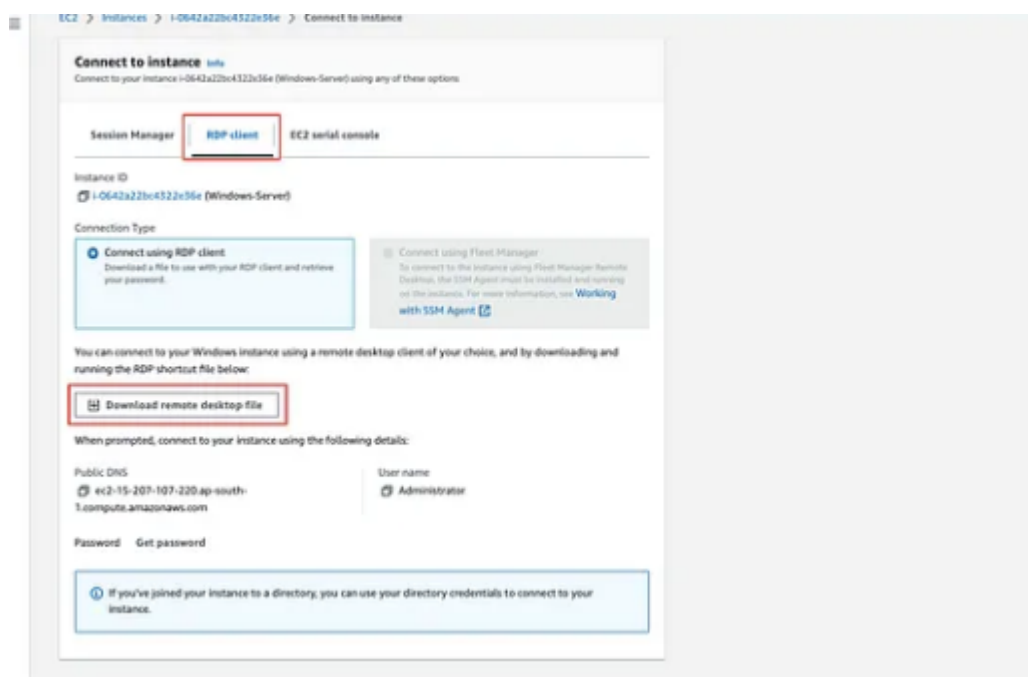
Now it's time to connect our Ec2 instance that we have recently launched.

**Step 8: Select your Windows Instance and Click on the “Connect”.**

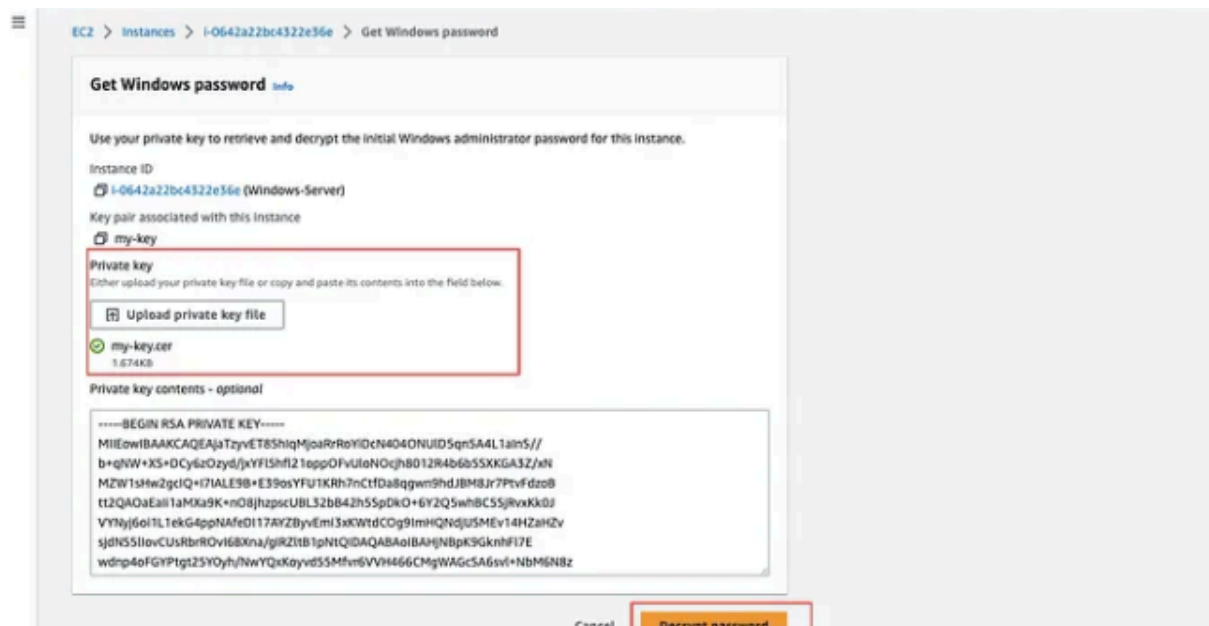


**Step 9: After Clicking on “Connect” the following interface will appear. just select the “RDP Client” Tab and download the “Remote desktop file”.**

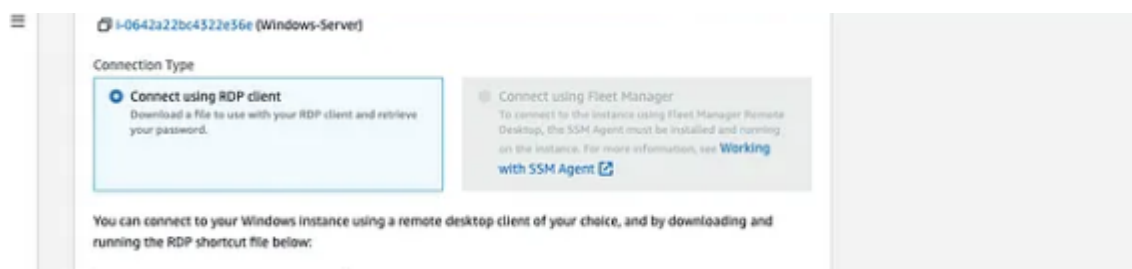
**Note: In the case of Windows only, Linux and mac have different mechanisms to connect RDP Connection.**



**Step 10: Now click on the “Get password”, select your “key pair” and decrypt the password.**

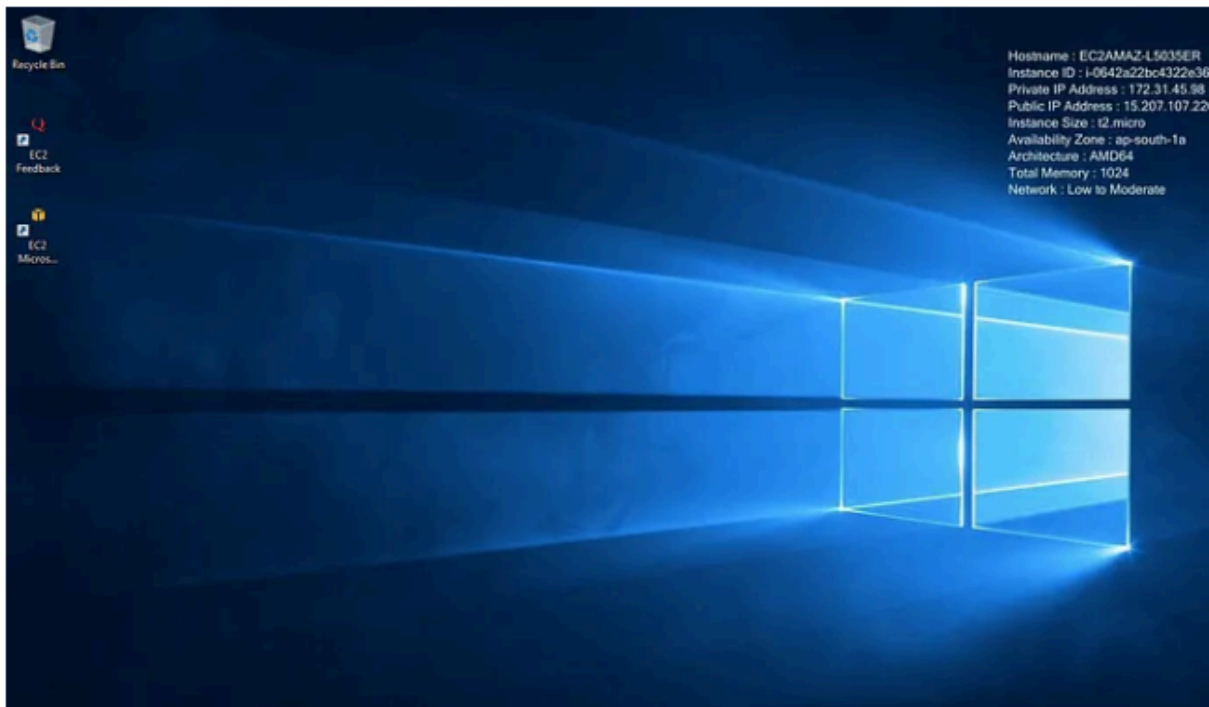


**Step 11: After clicking on the “Decrypt password” the following interface will appear to copy the password and use that password to connect your Windows EC2 instance**



**Step 12: Open your Downloaded file “RDP file” and put, the password that you decrypted.**

The default user name will be “Administrator” and the password is that you have decrypted and shown in the above screenshot.



**Note:** If you are getting continuous getting security pop while accessing browser in aws , search local server & off the enhance security feature .