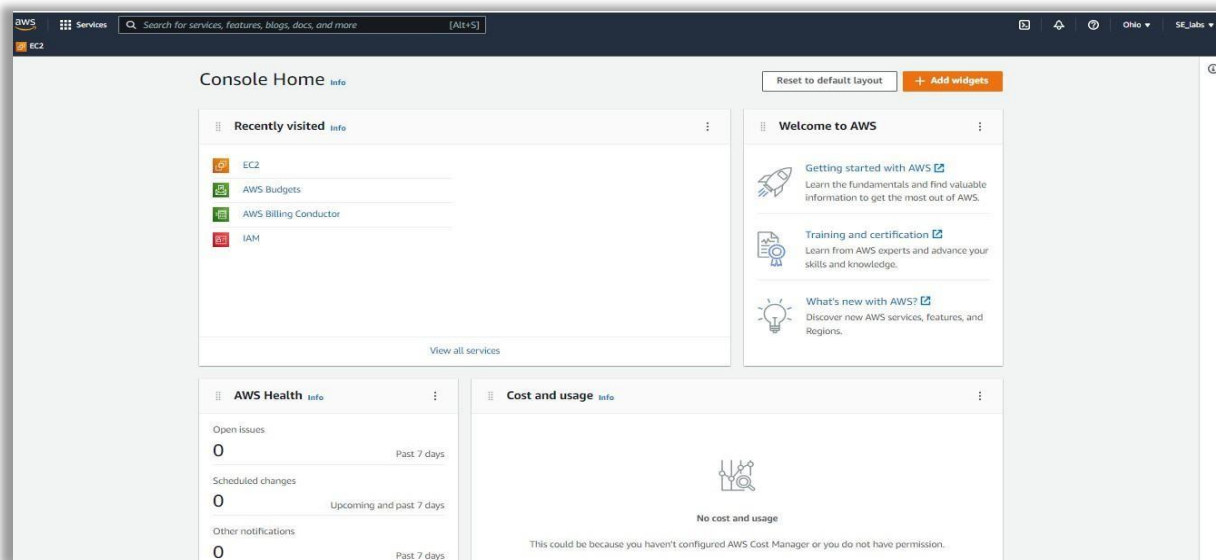
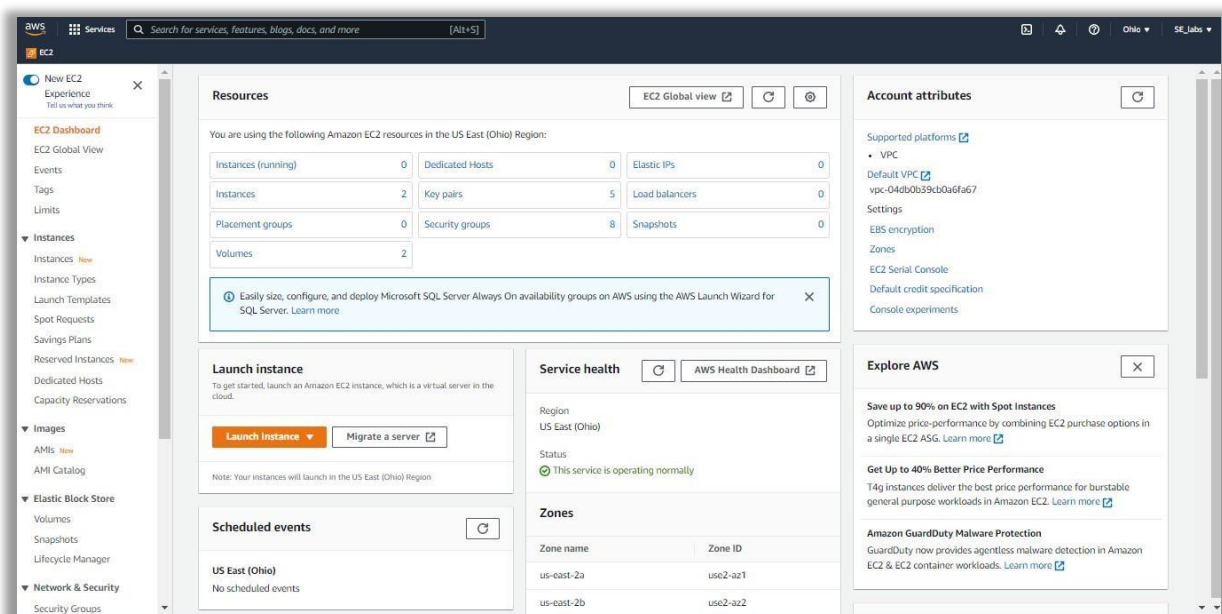


Follow the Below Steps to Configure Tenable Nessus Vulnerability Scanner in AWS

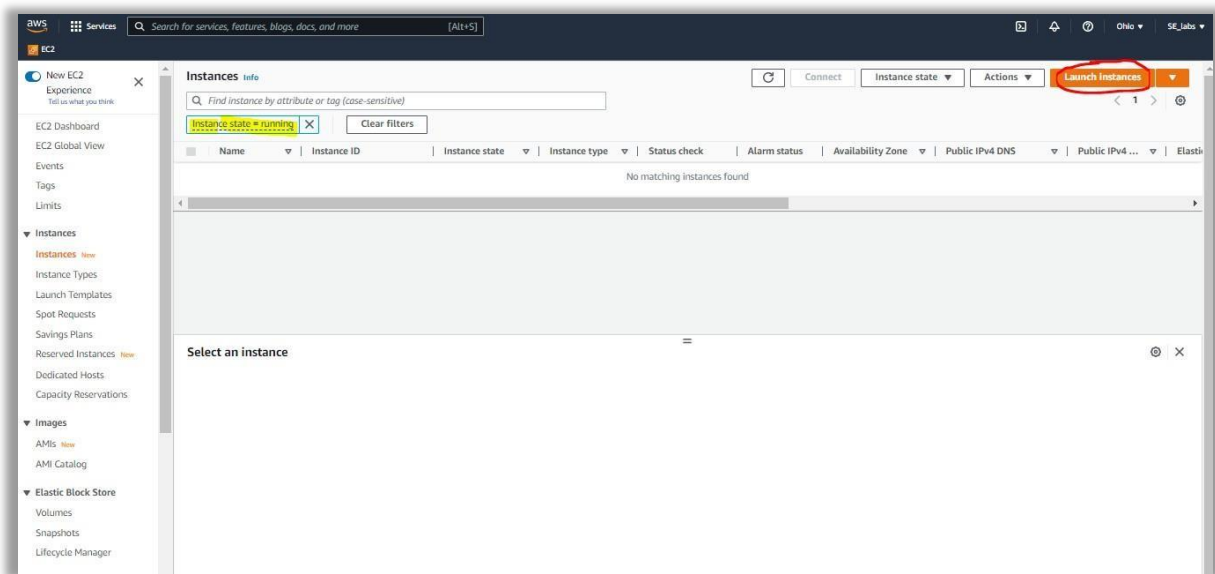
1. After you login into AWS Console you should be able to see below screen. Then click or search for EC2 in search dialogue and **select Ohio Region** in top right corner



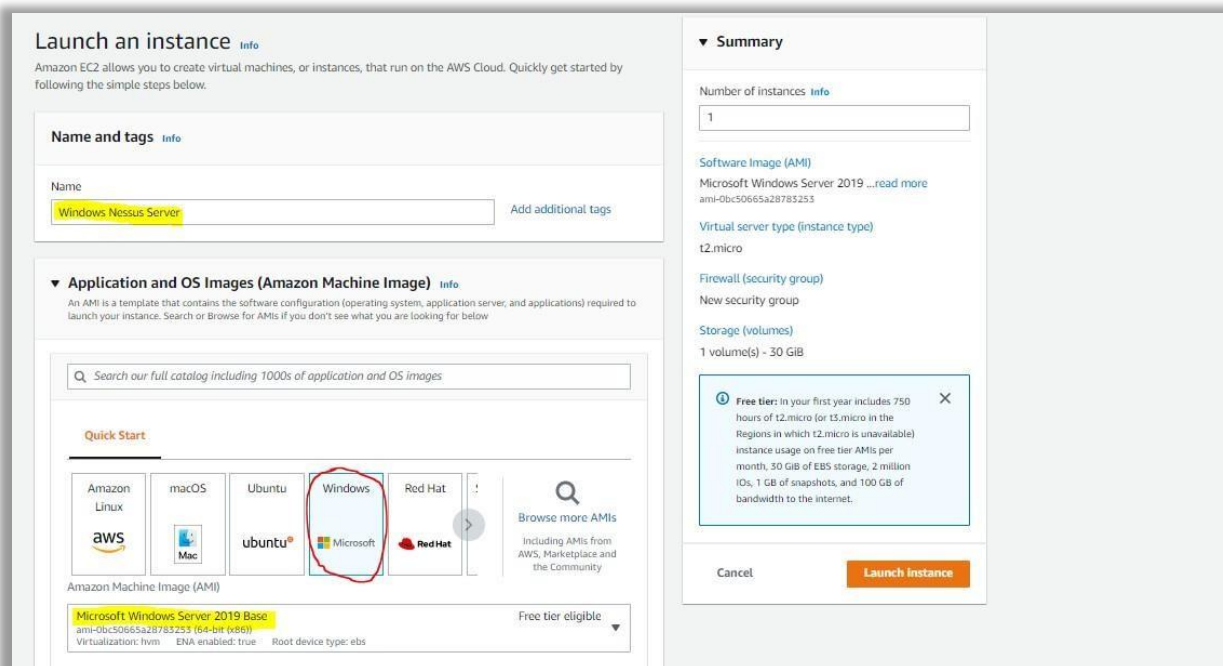
2. Once clicked on EC2 you should be able to see below screen and make sure you have selected Ohio region on top right



3. Click on Launch Instance tab on top right corner as marked in below image to spin up new server.

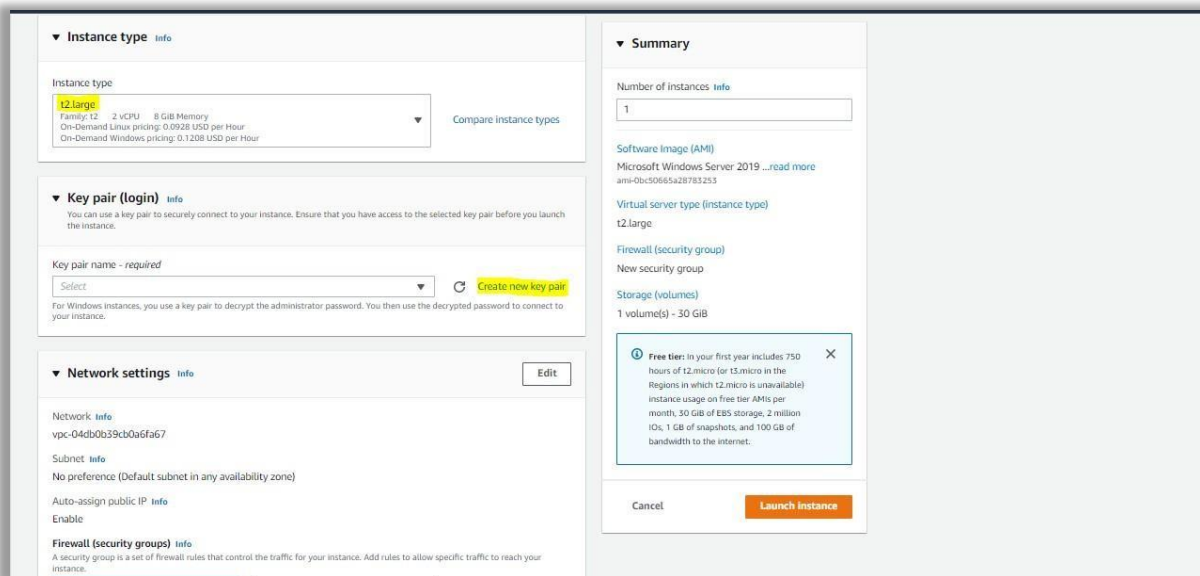


4. To spin up a Windows Server provide the below details as shown in Image and select **windows** Machine as AMI with Microsoft **Windows Server 2019 Base**

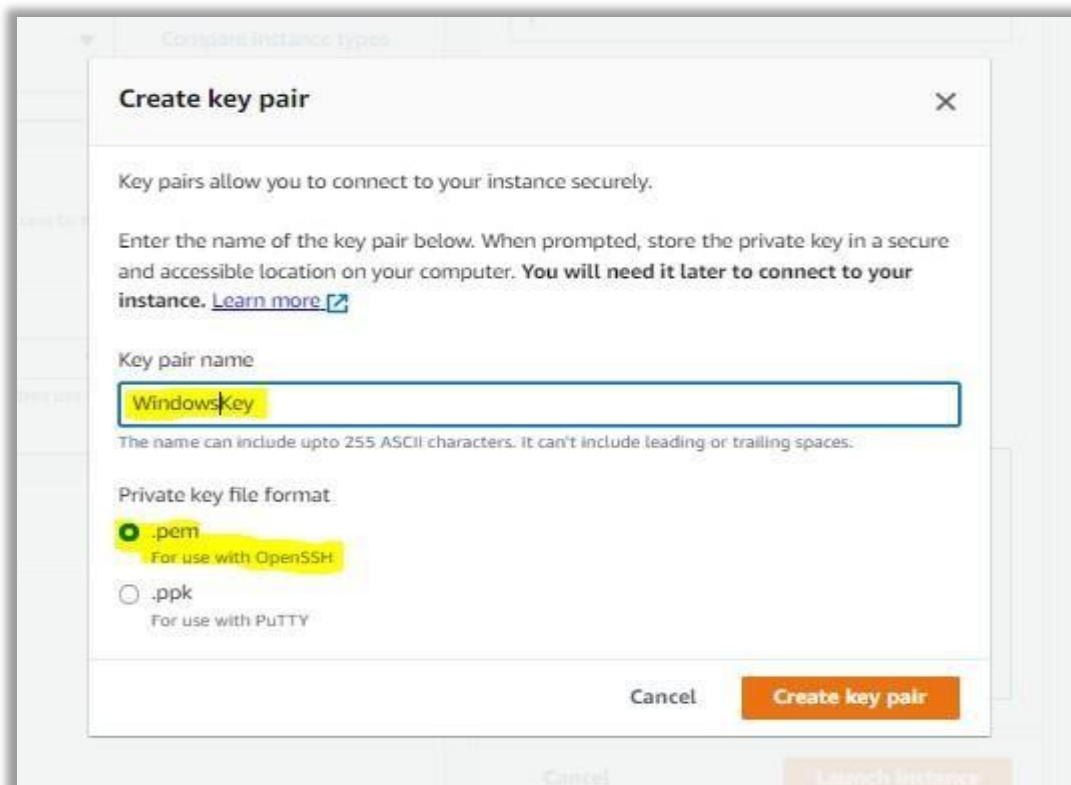


5. Select T2 Large as your Instance Type and click on Create new key pair.

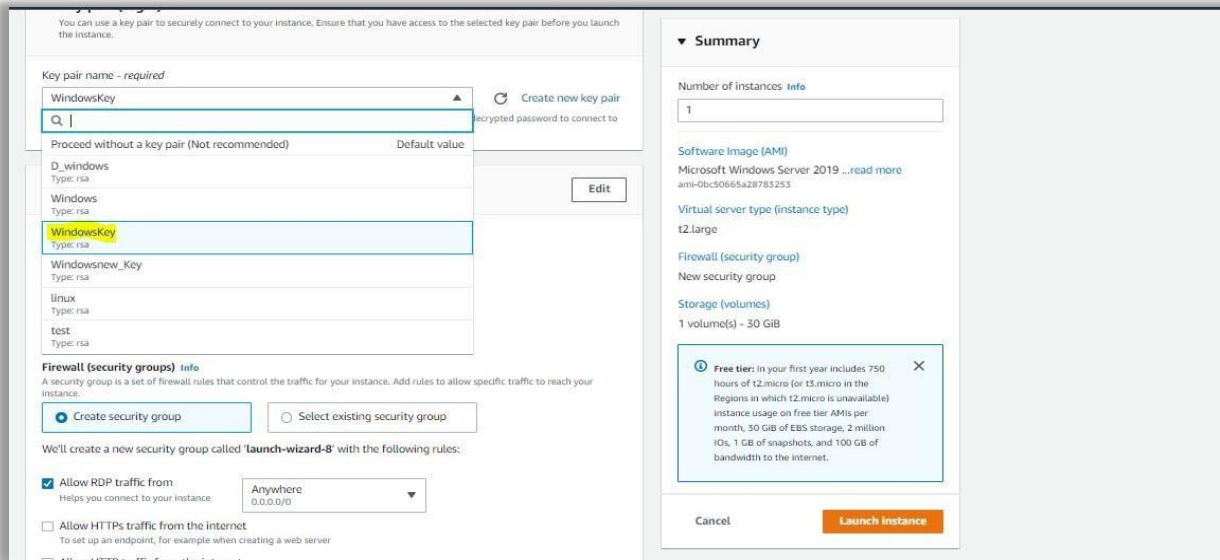
Note: On selecting T2 Large AWS will start charging for your usage. Even you can select T2 Micro which is free but you experience lot more slower to work



6. Provide the key pair name as windows key and select .pem as key pair



7. Select the Key pair name that you have given in previous step and select the steps as it in image.



You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key before you launch the instance.

Key pair name - required

WindowsKey

Create new key pair

Proceed without a key pair (Not recommended) Default value

Edit

WindowsKey

Windowsnew_Key

linux

test

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

We'll create a new security group called 'launch-wizard-8' with the following rules:

Allow RDP traffic from

Anywhere

Allow HTTP traffic from the internet

Summary

Number of instances Info

1

Software Image (AMI)

Microsoft Windows Server 2019 ...read more

Virtual server type (instance type)

t2.large

Firewall (security group)

New security group

Storage (volumes)

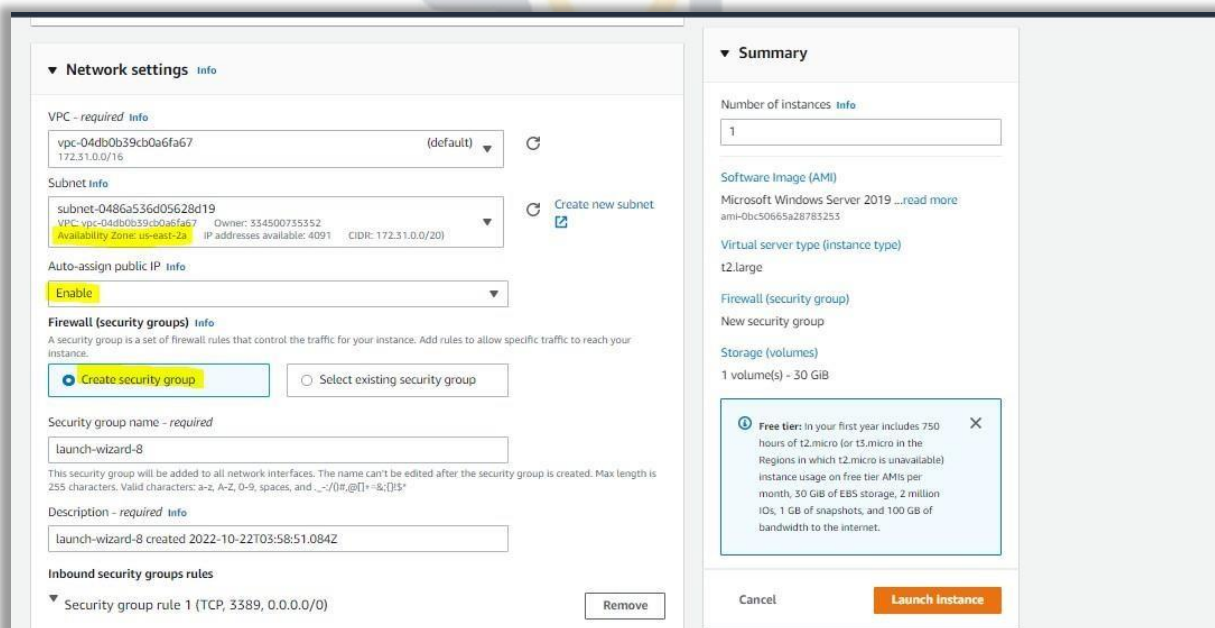
1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

8. Remember all our instances need to be spin up in same subnet so carefully select the same subnet whenever you spin a new instance.



Network settings Info

VPC - required Info

vpc-04db0b39cb0a6fa67 (default)

Subnet Info

subnet-0486a536d05628d19

Create new subnet

Auto-assign public IP Info

Enable

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

Security group name - required

launch-wizard-8

Description - required Info

launch-wizard-8 created 2022-10-22T03:58:51.084Z

Inbound security groups rules

Security group rule 1 (TCP, 3389, 0.0.0.0/0)

Remove

Summary

Number of instances Info

1

Software Image (AMI)

Microsoft Windows Server 2019 ...read more

Virtual server type (instance type)

t2.large

Firewall (security group)

New security group

Storage (volumes)

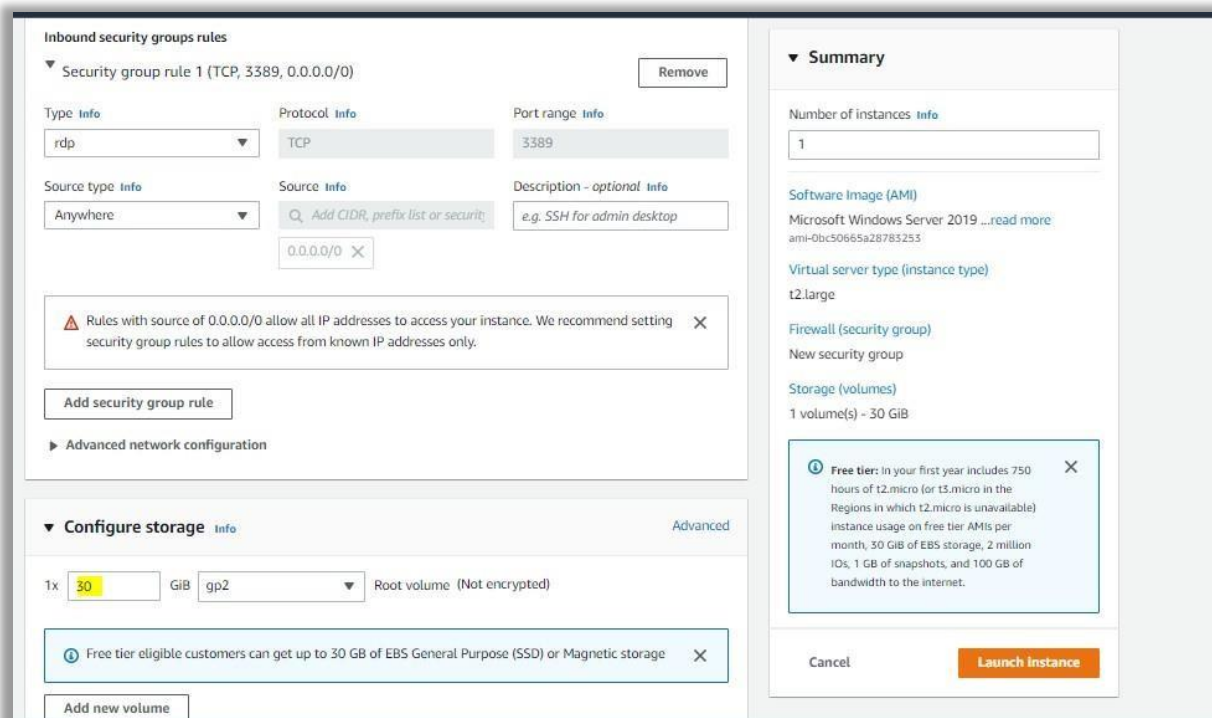
1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

9. To open the ports select the below configurations.



The screenshot shows the AWS console interface for configuring an inbound security group rule. The rule is named "Security group rule 1 (TCP, 3389, 0.0.0.0/0)". The configuration is as follows:

- Type:** rdp
- Protocol:** TCP
- Port range:** 3389
- Source type:** Anywhere
- Source:** 0.0.0.0/0
- Description - optional:** e.g. SSH for admin desktop

A warning message states: "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." Below this, there is a button "Add security group rule" and a link "Advanced network configuration".

The "Configure storage" section shows:

- 1x:** 30 GiB
- gp2:** Root volume (Not encrypted)

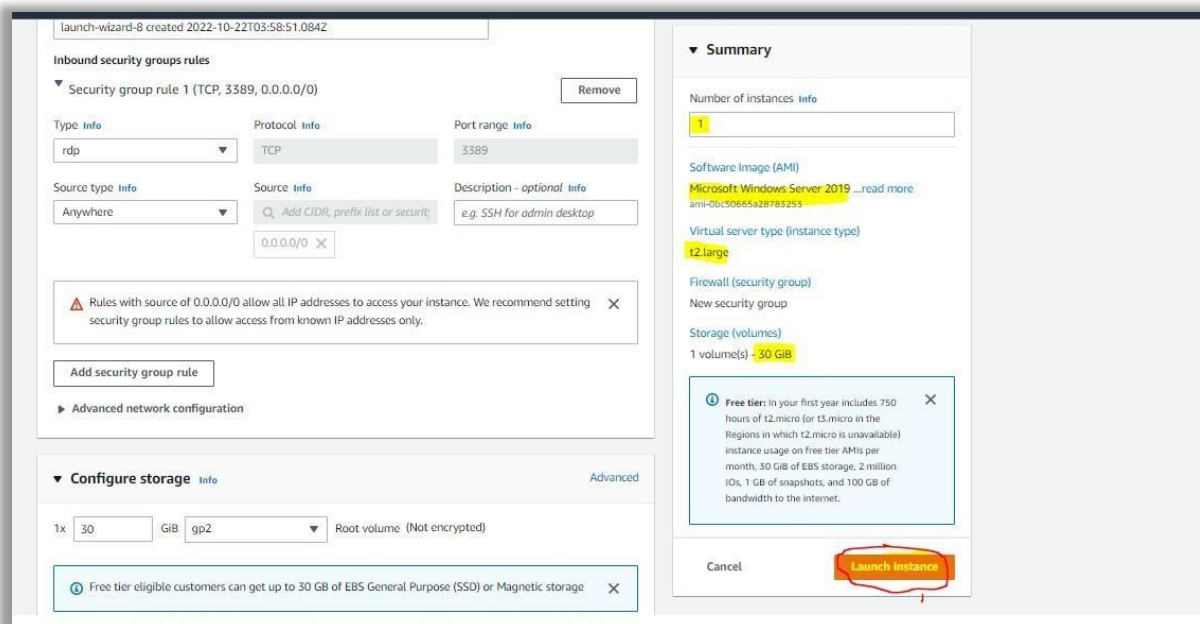
A note indicates: "Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage".

The "Summary" section on the right shows:

- Number of instances:** 1
- Software Image (AMI):** Microsoft Windows Server 2019 ...read more
- Virtual server type (instance type):** t2.large
- Firewall (security group):** New security group
- Storage (volumes):** 1 volume(s) - 30 GiB

At the bottom right, there is a "Launch instance" button and a "Cancel" button.

10. Review above steps and click on Launch Instances button.

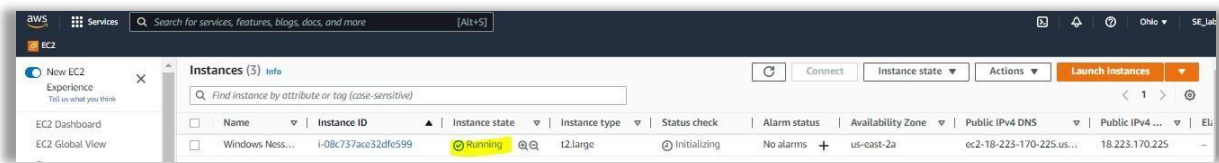


This screenshot is similar to the previous one, showing the same configuration for the inbound security group rule and storage. However, the "Launch instance" button in the summary section is highlighted with a red circle and a red arrow, indicating the next step in the process.

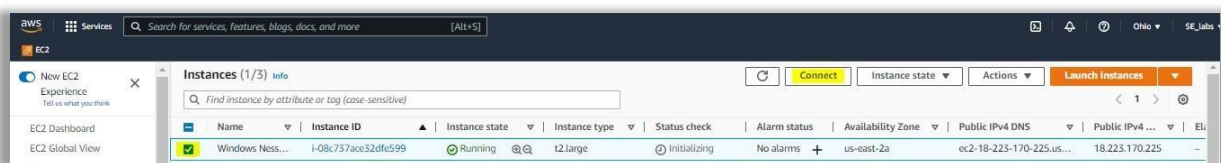
Gateway to Cybersecurity Careers



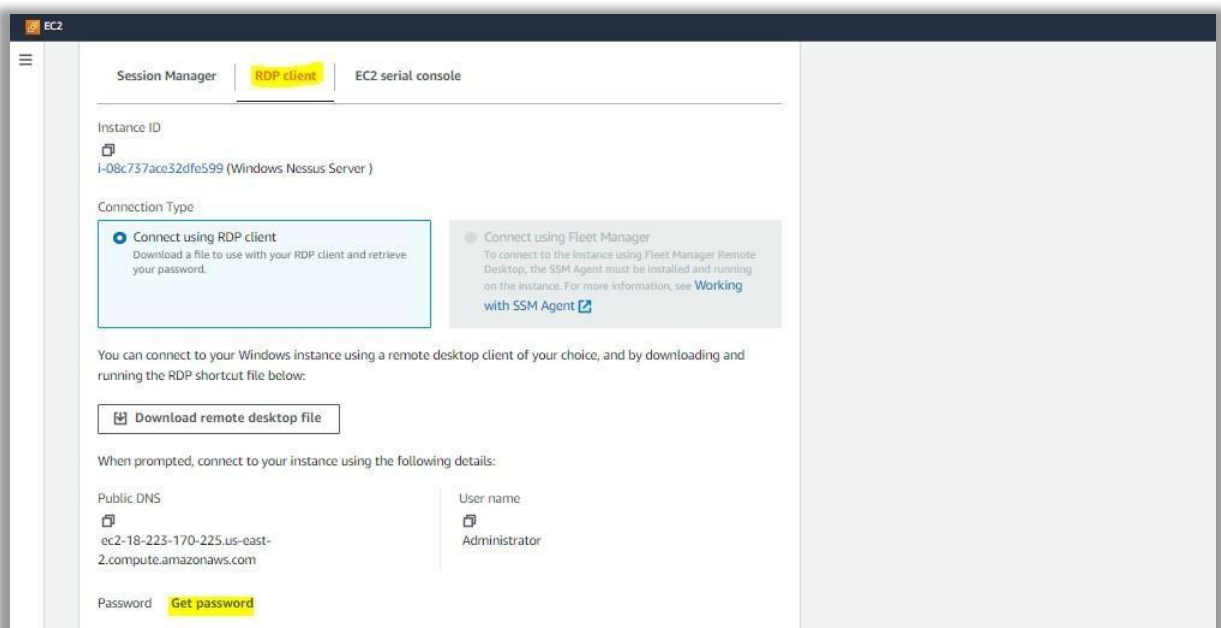
11. Verify whether the Instances are running or not.



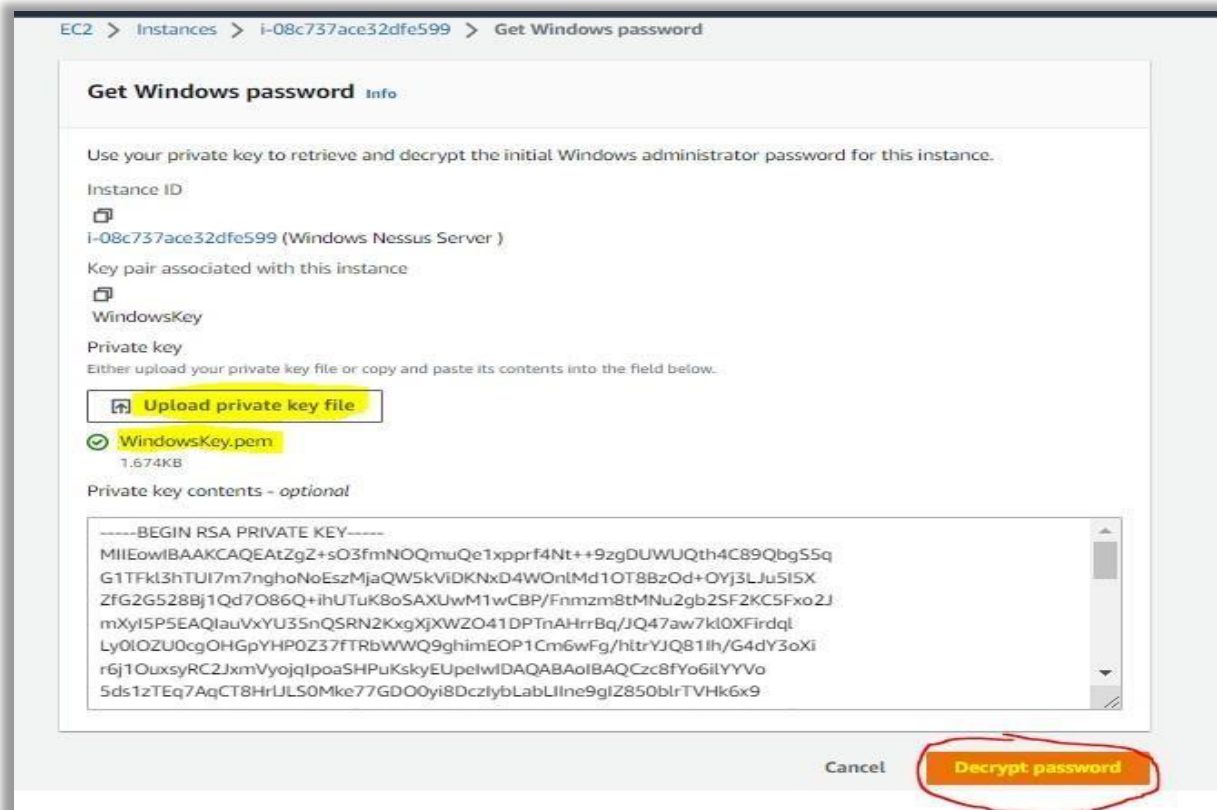
12. Click on Connect button to Login to that Instance



13. Select RDP Client and click on Get password button



14. Click on Upload private Key file and Select the file that has been previously downloaded on step No 7 and click on Decrypt Password.



EC2 > Instances > i-08c737ace32dfe599 > Get Windows password

Get Windows password Info

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID
i-08c737ace32dfe599 (Windows Nessus Server)

Key pair associated with this instance
WindowsKey

Private key
Either upload your private key file or copy and paste its contents into the field below.

Upload private key file

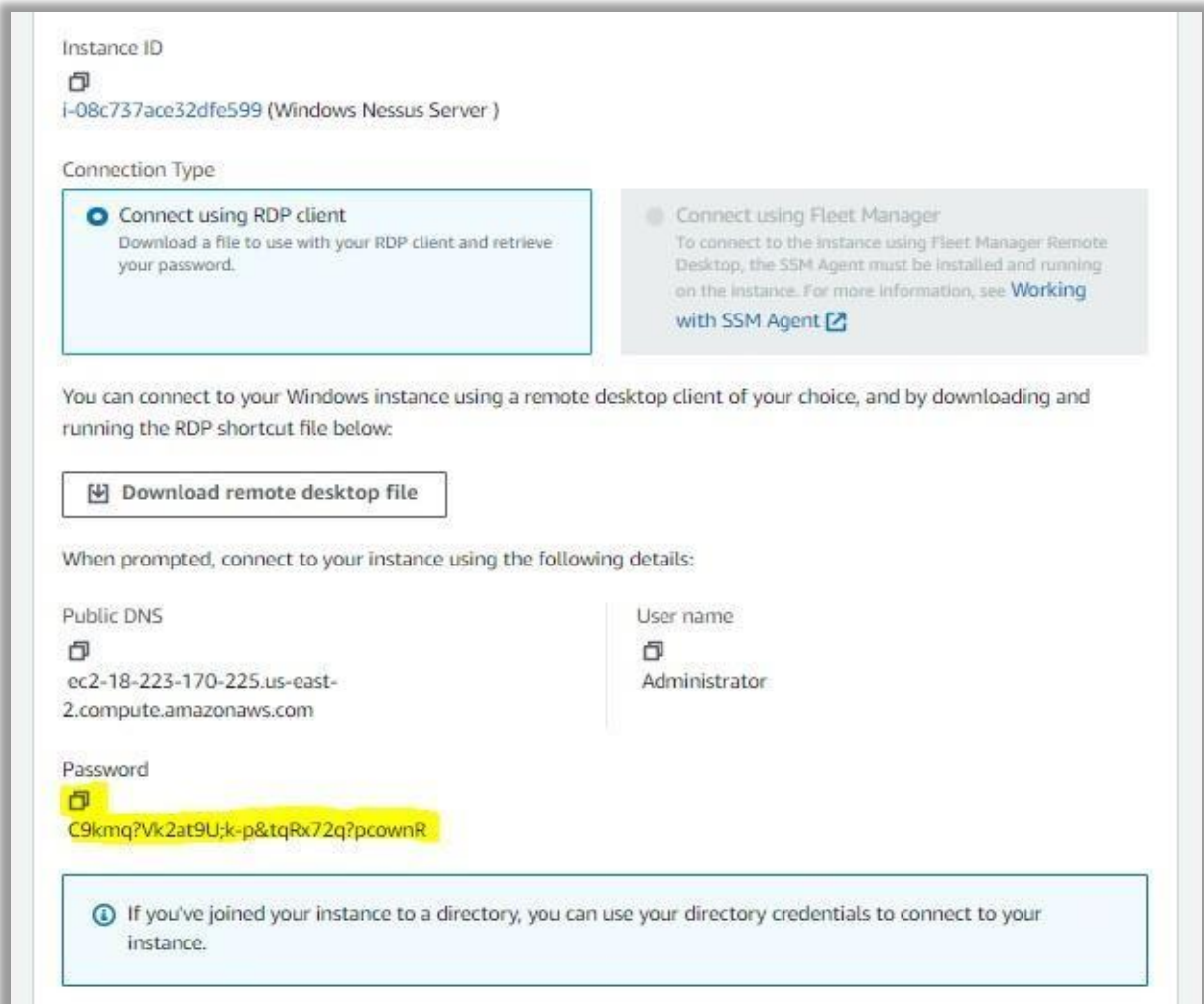
✓ WindowsKey.pem
1.674KB

Private key contents - optional

```
-----BEGIN RSA PRIVATE KEY-----
MIIIEowIBAACAQEAtZgZ+sO3fmNOQmuQe1xprrf4Nt++9zgDUWUQth4C89QbgSSq
G1TFkl3hTUI7m7nghoNoEszMjaQW5kVIDKNxD4WOnlMd1OT8BzOd+OYj3LJu5ISX
ZfG2G528Bj1Qd7O86Q+ihUTuK8oSAXUwM1wCBP/Fnmzm8tMNU2gb2SF2KC5Fxo2J
mXyI5P5EAQlauVxYU35nQSRN2KxgXjXWZO41DPTnAHrrBq/JQ47aw7kl0XFirdql
Ly0lOZU0cgOHGpYHP0Z37FTRbWWQ9ghimEOP1Cm6wFg/hltrYJQ81lh/G4dY3oXi
r6j1OuxsyRC2JxmVyojlpoaSHPuKskyEUpeIwIDAQABAoIBAQCzc8FYo6ilYYVo
Sds1zTEq7AqCT8HrJULS0Mke77GDO0yi8DczlybLabLIIne9gJZ850blrTVHk6x9
-----
```

Cancel **Decrypt password**

15. Copy the Password that you have got after following step No 14.



Instance ID
i-08c737ace32dfe599 (Windows Nessus 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 details:

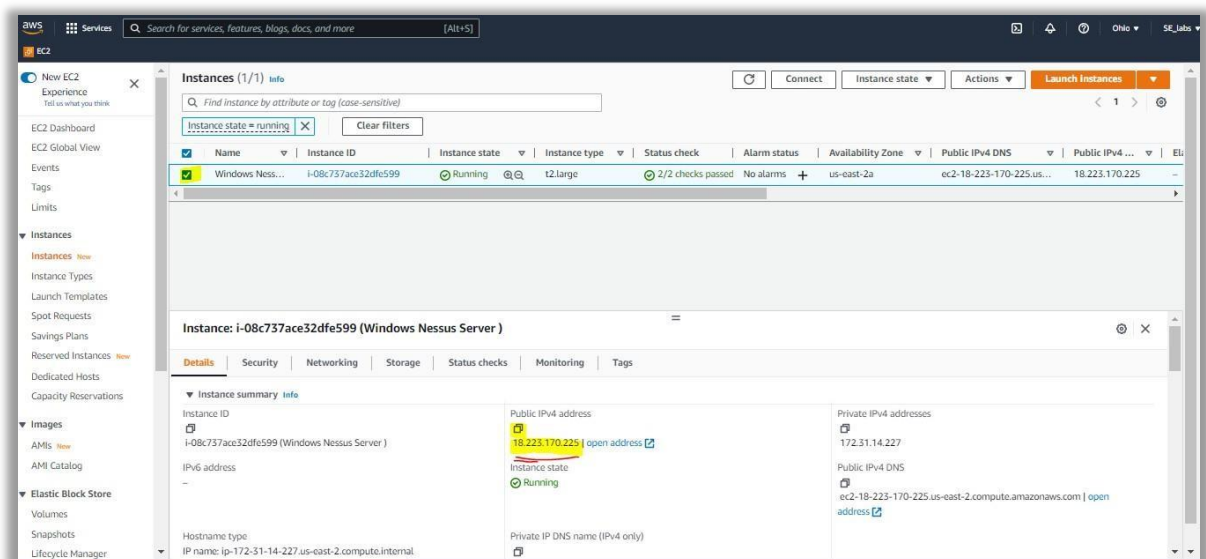
Public DNS
ec2-18-223-170-225.us-east-2.compute.amazonaws.com

User name
Administrator

Password
C9kmg?Vk2at9U;k-p&tgRx72q?pcownR

[If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.](#)

16. Come back to Instances page and Copy the Public IP of your Instance.



Instances (1/1) info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
Windows Ness...	i-08c737ace32dfe599	Running	t2.large	2/2 checks passed	No alarms	us-east-2a	ec2-18-223-170-225.us...	18.223.170.225

Instance: i-08c737ace32dfe599 (Windows Nessus Server)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary info

Instance ID
i-08c737ace32dfe599 (Windows Nessus Server)

Public IPv4 address
18.223.170.225 | [open address](#)

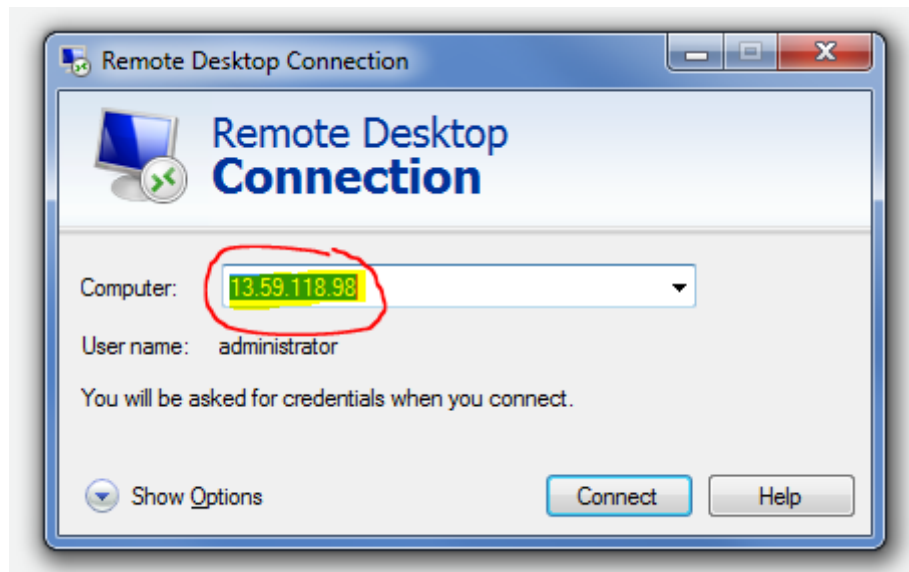
Private IPv4 addresses
172.31.14.227

Public IPv4 DNS
ec2-18-223-170-225.us-east-2.compute.amazonaws.com | [open address](#)

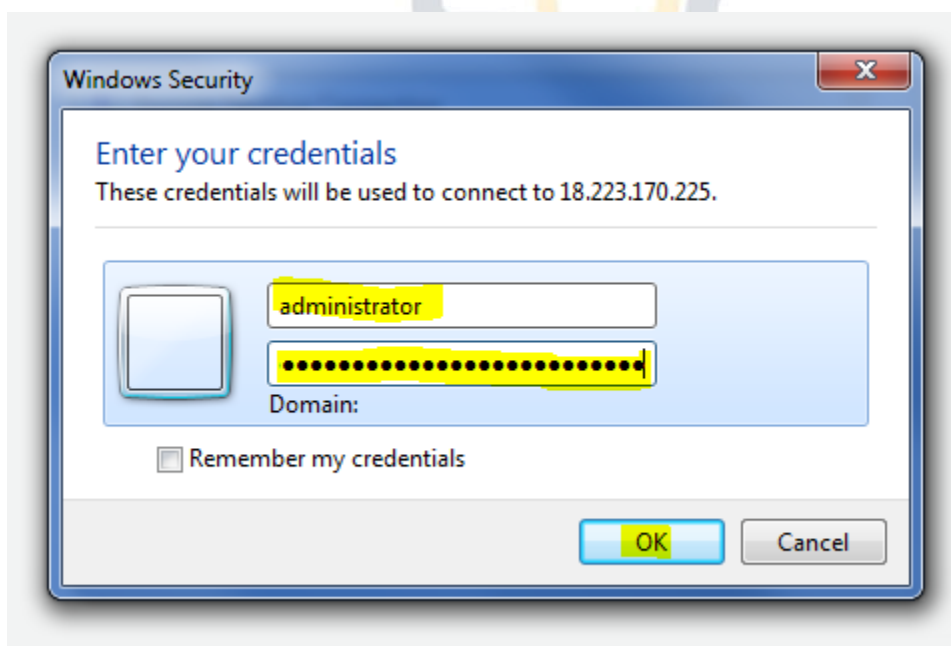
Instance state
Running

Private IP DNS name (IPv4 only)

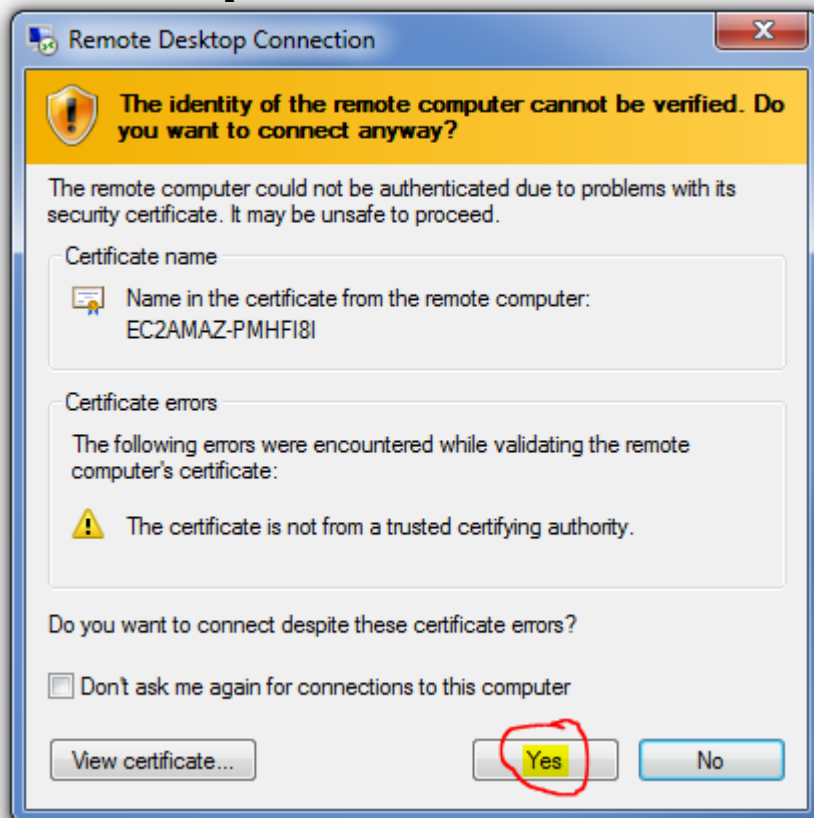
17. Open Remote Desktop Connection from Start Menu and paste the IP that you have copied from step No 16 and click on connect button.



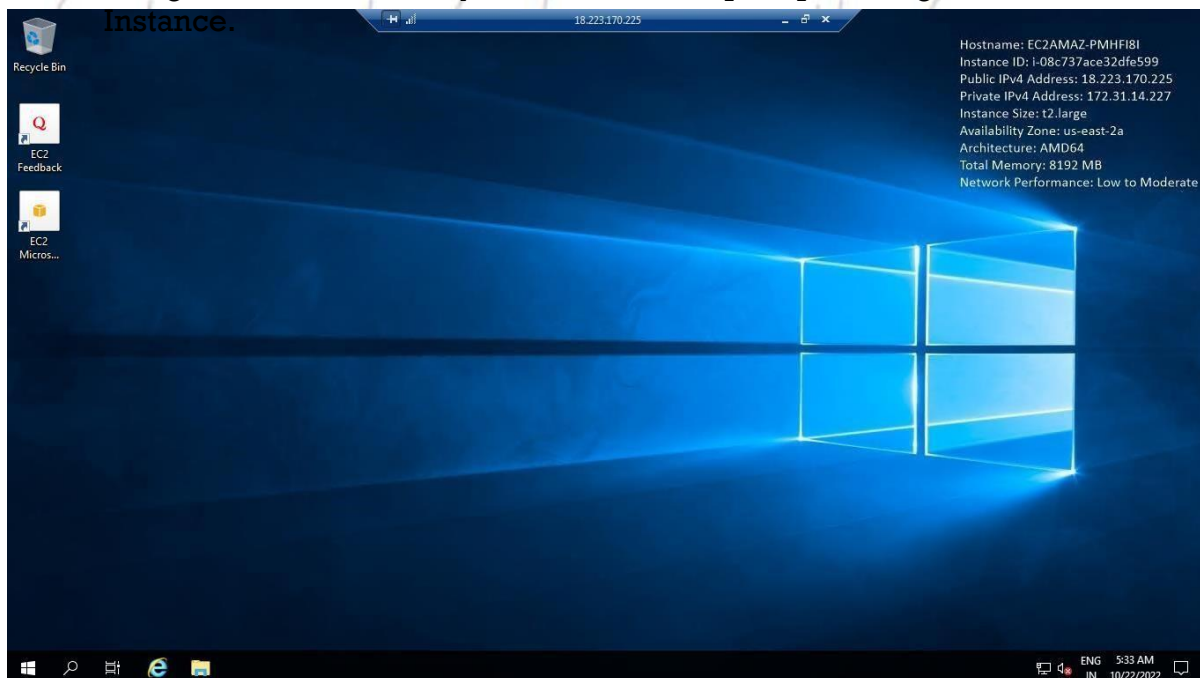
18. Type in administrator as username and paste the password that you have copied at step No 15.



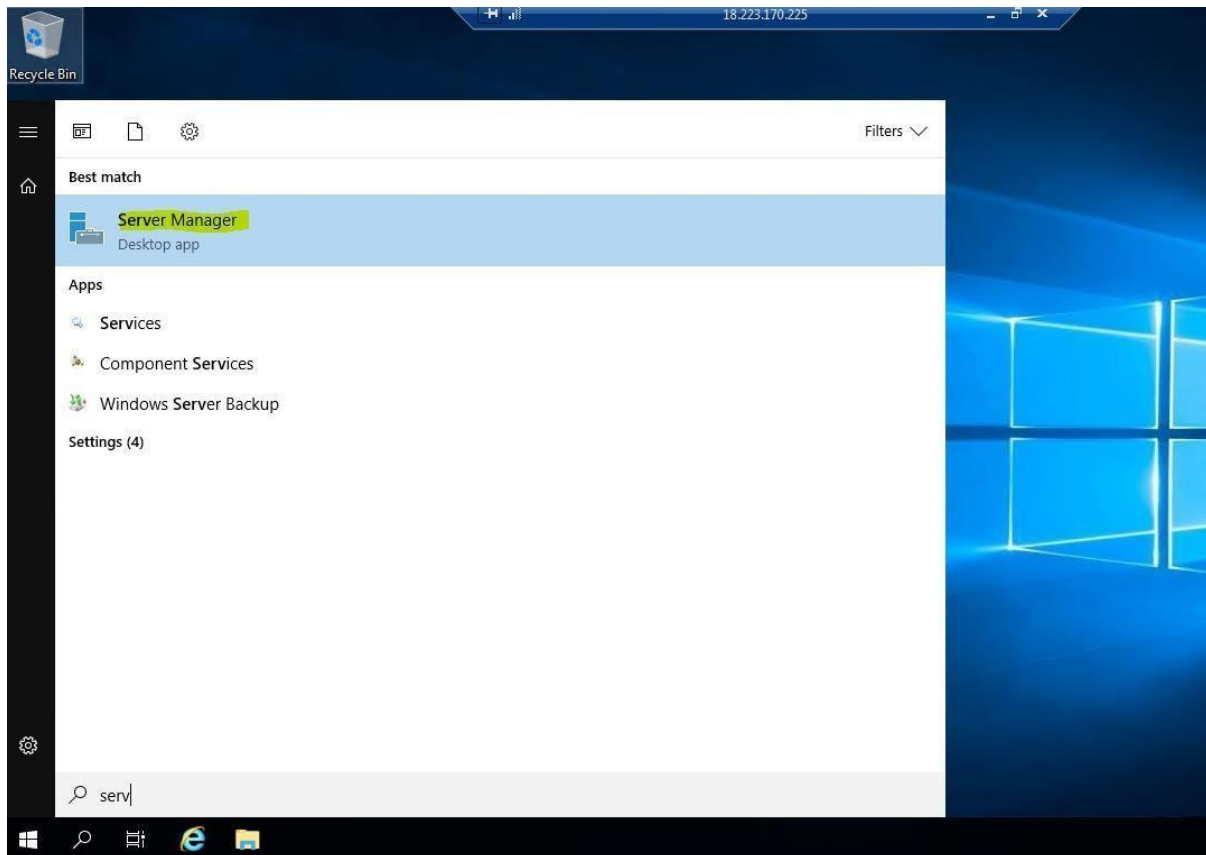
19. Click on Yes after Step No 18



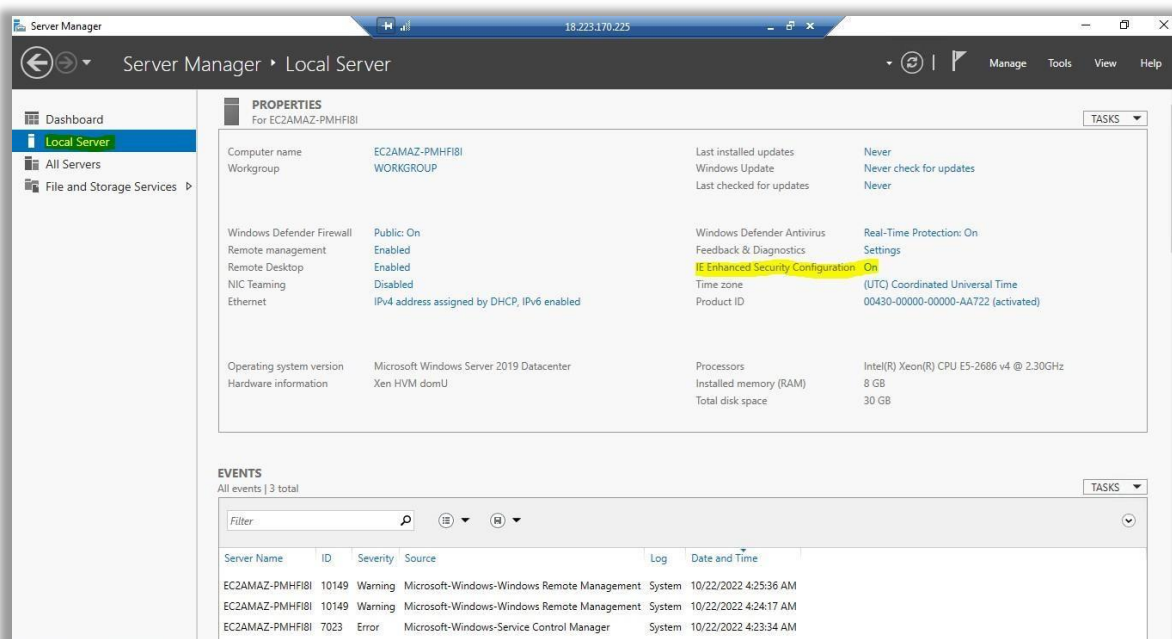
20. Congratulations...!! Now you were able to spin up and login into Windows Instance.



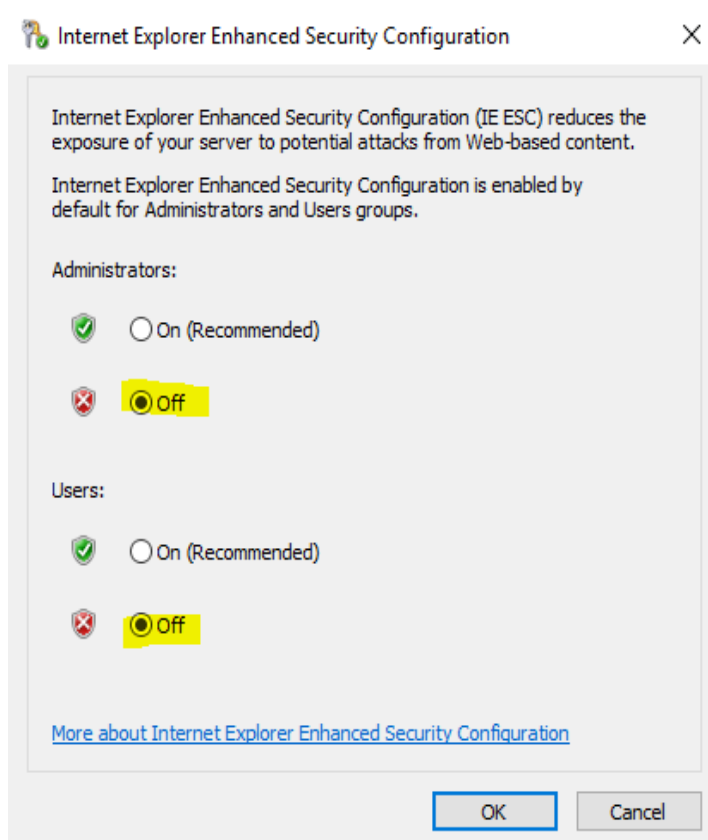
21. After successfully logging into Windows Instance need to do some changes in the settings Goto Start>type server manager



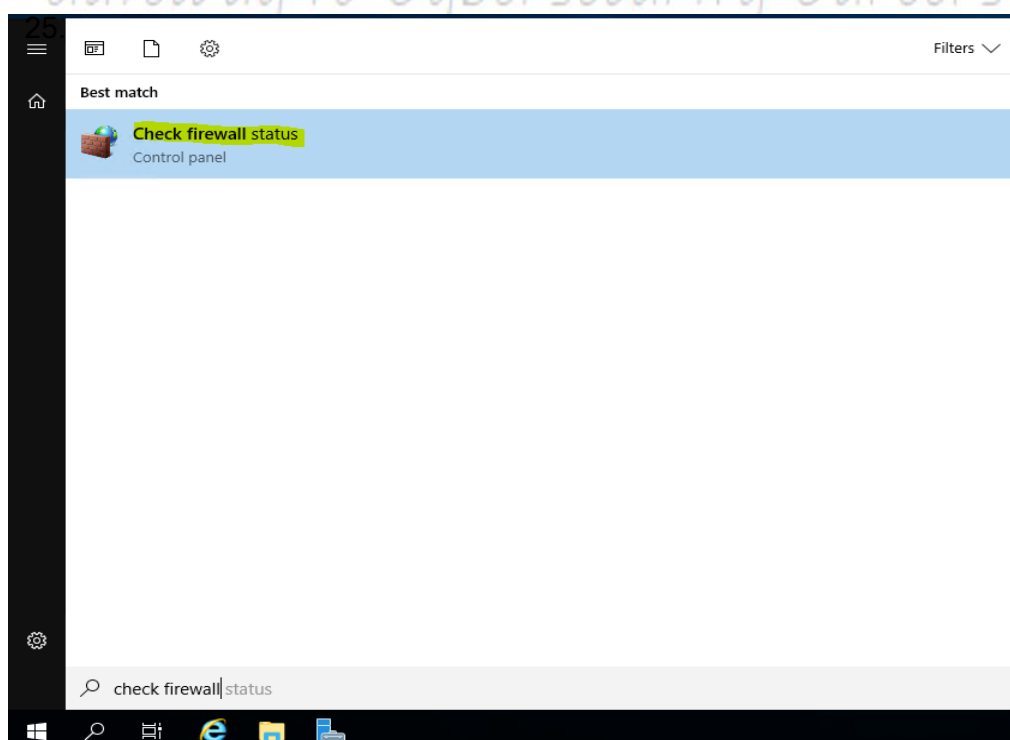
22. Select Local Server in left hand side and check for IE Enhanced Security Configuration options as shown in Image.



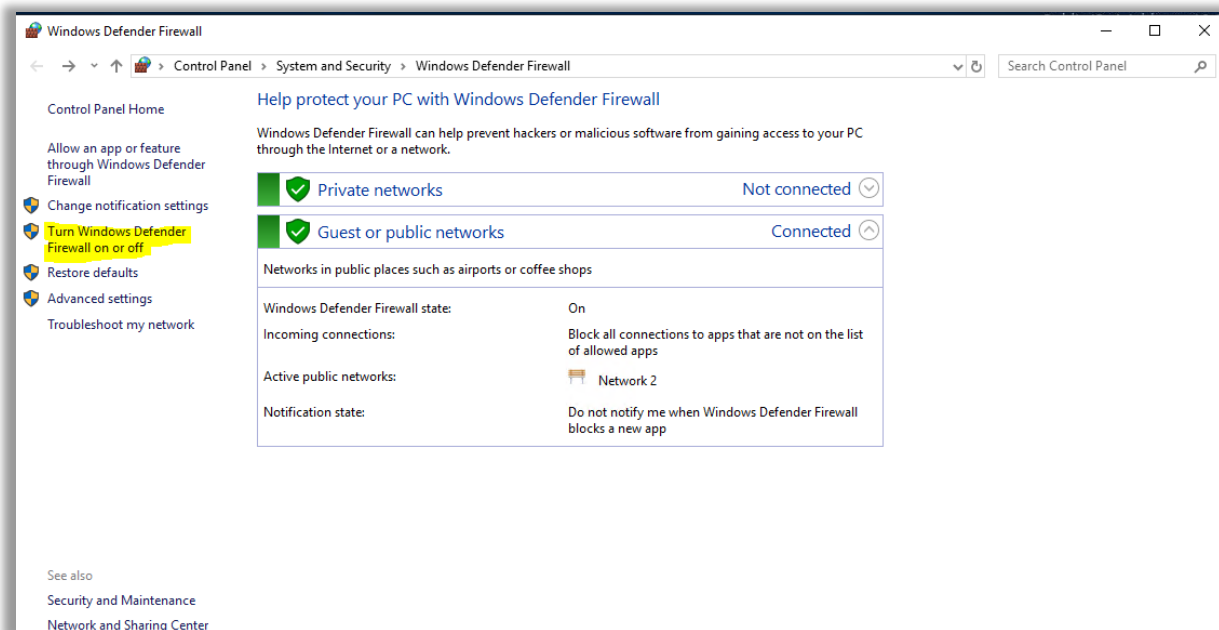
23. Click on IE Enhanced Security Configuration and Turn off both Administrator and Users as shown in image.



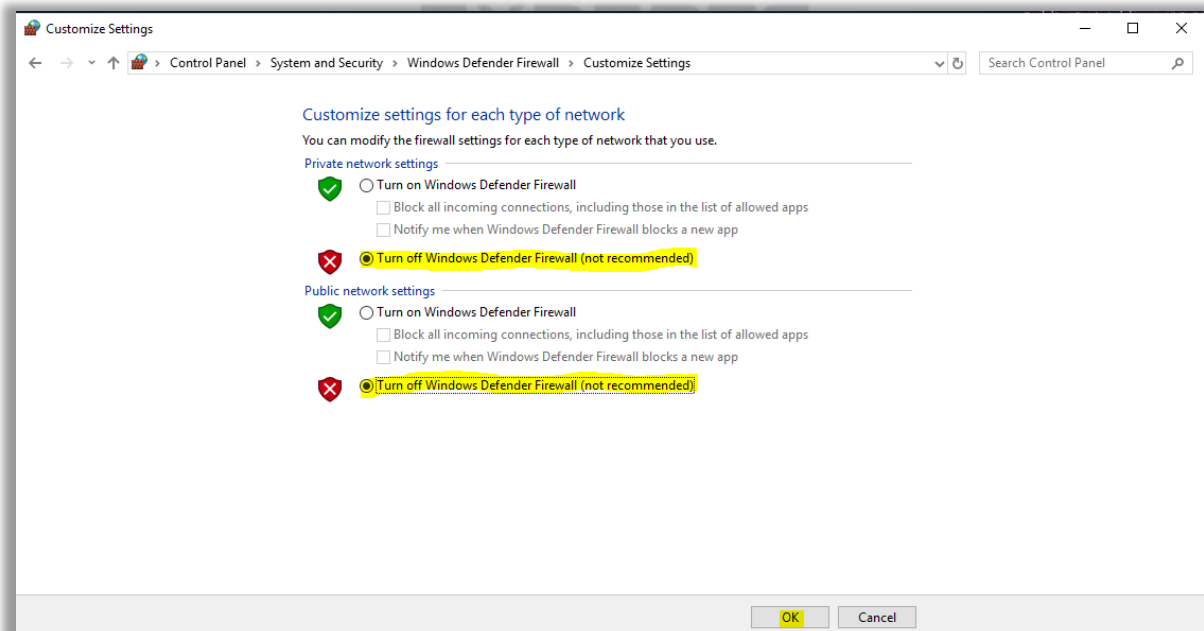
24. The Host Firewall running in the Server might not be allowing few of the features to access so need to turn off the firewall go to start > type check firewall status and Click



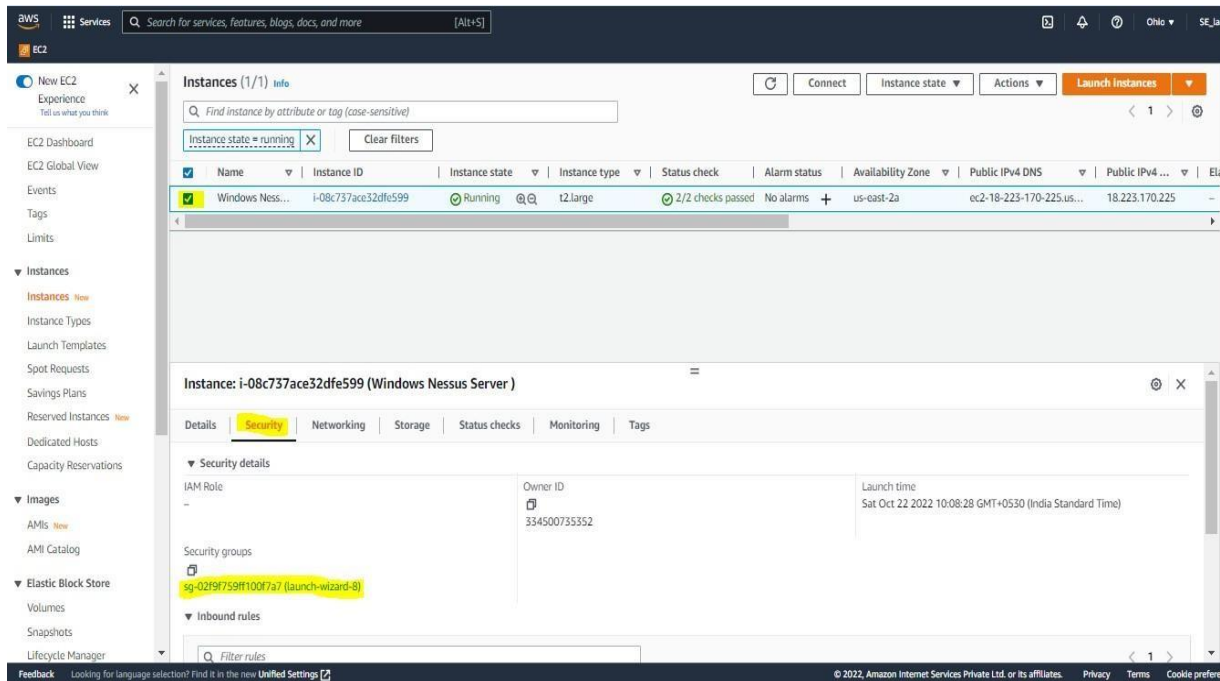
25. From left hand side panel select Turn Windows Defender Firewall on or off as shown in below Image



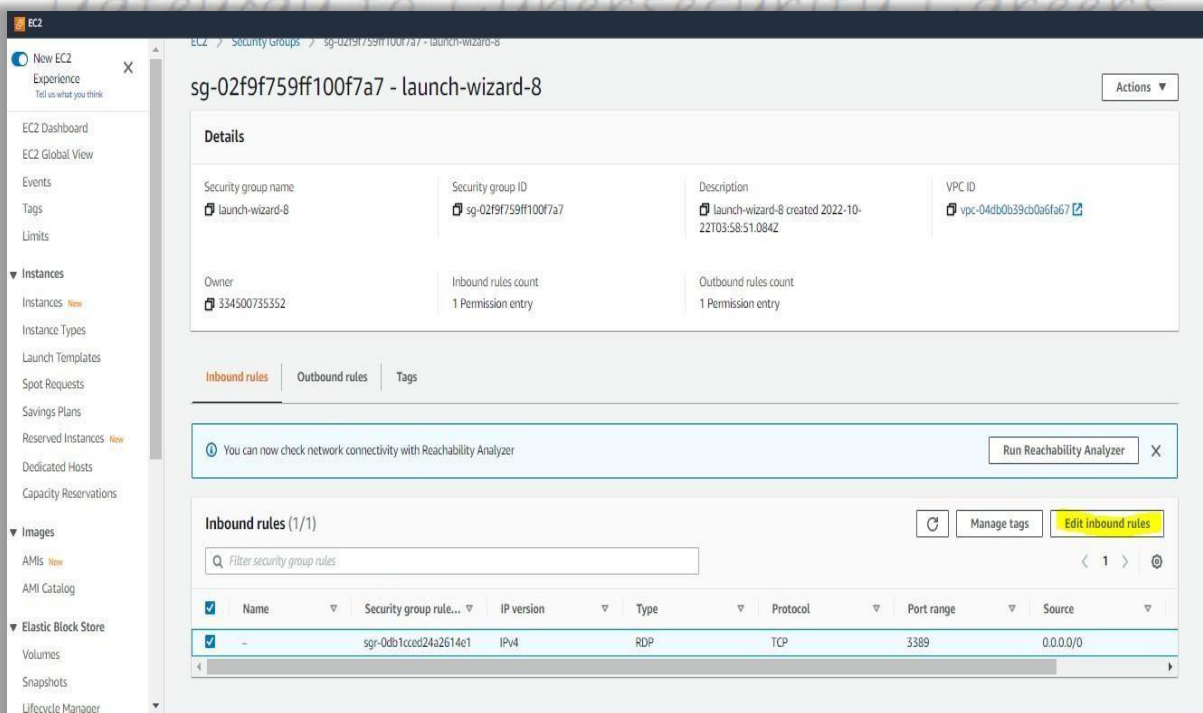
26. Select the options Turn Off Windows Defender Firewall



27. Now we need to open few of the ports for our Communication purpose



28. Then Click on Inbound Rules.



29. Open the below ports for further communication 8834 and 0-65535

EC2 > Security Groups > sg-02f9f759ff100f7a7 - launch-wizard-8 > Edit inbound rules

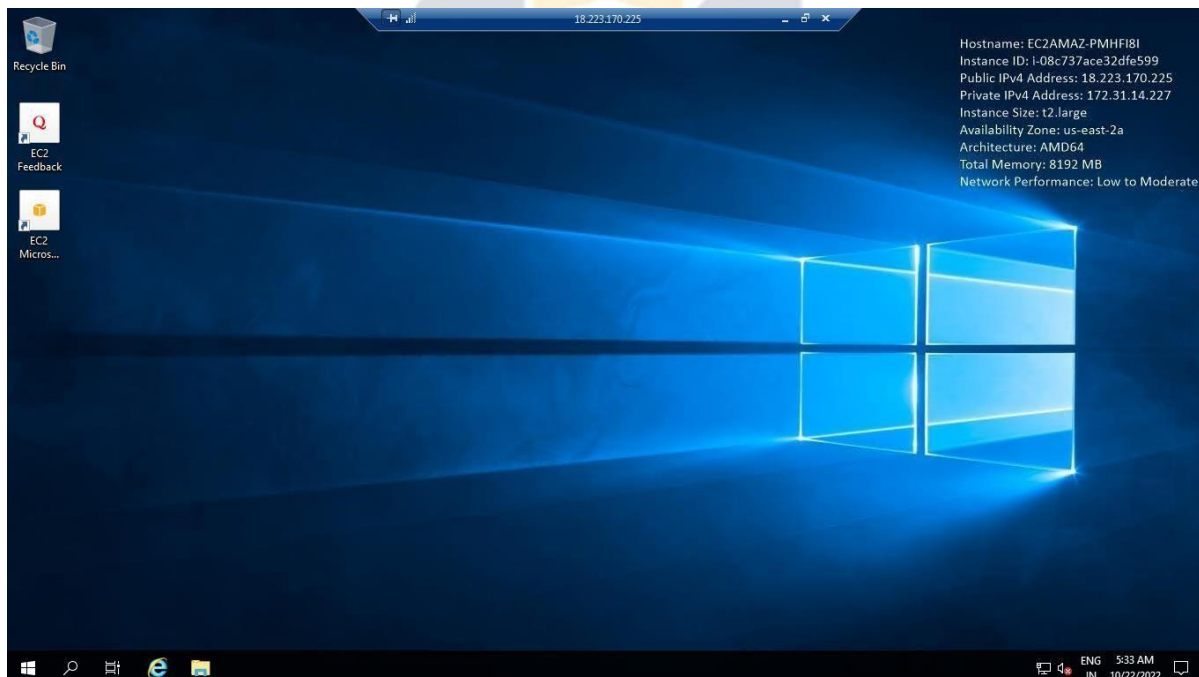
Edit inbound rules info

Inbound rules control the incoming traffic that's allowed to reach the instance.

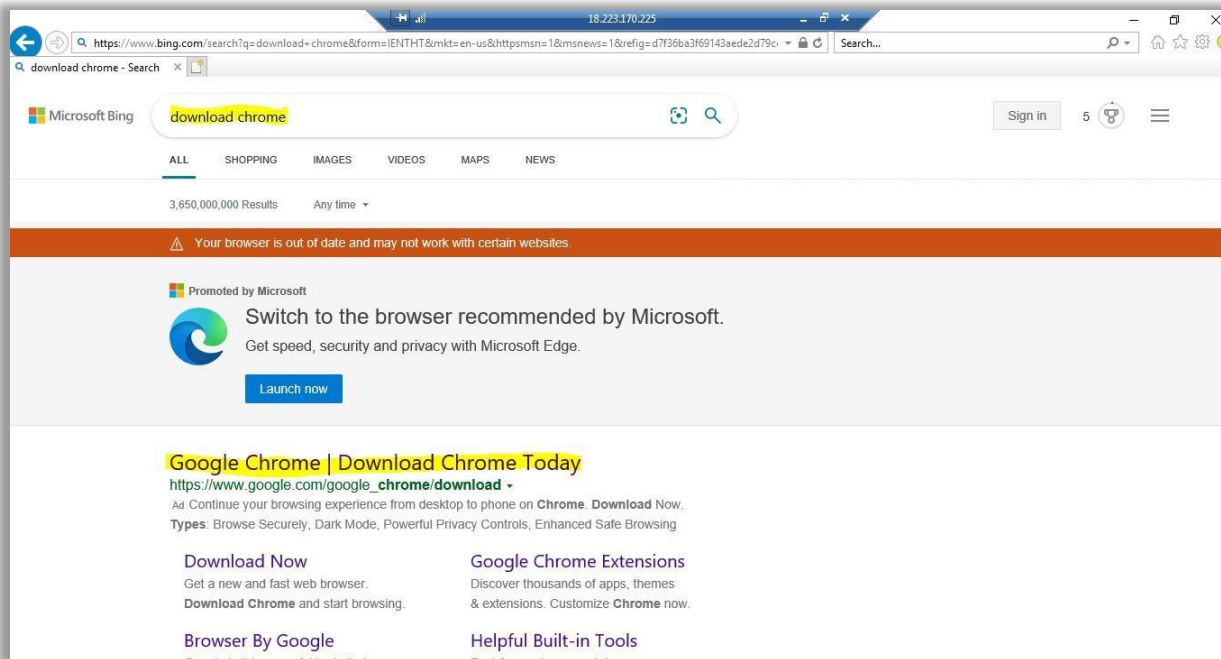
Inbound rules info

Security group rule ID	Type <small>info</small>	Protocol <small>info</small>	Port range <small>info</small>	Source <small>info</small>	Description - optional <small>info</small>	
sg-r-0db1cccd24a2614e1	RDP	TCP	3389	Custom	<input type="text" value="Q"/>	<input type="button" value="Delete"/>
-	All TCP	TCP	0 - 65535	Anywhere...	<input type="text" value="Q"/>	<input type="button" value="Delete"/>
-	Custom TCP	TCP	8834	Anywhere...	<input type="text" value="Q"/>	<input type="button" value="Delete"/>

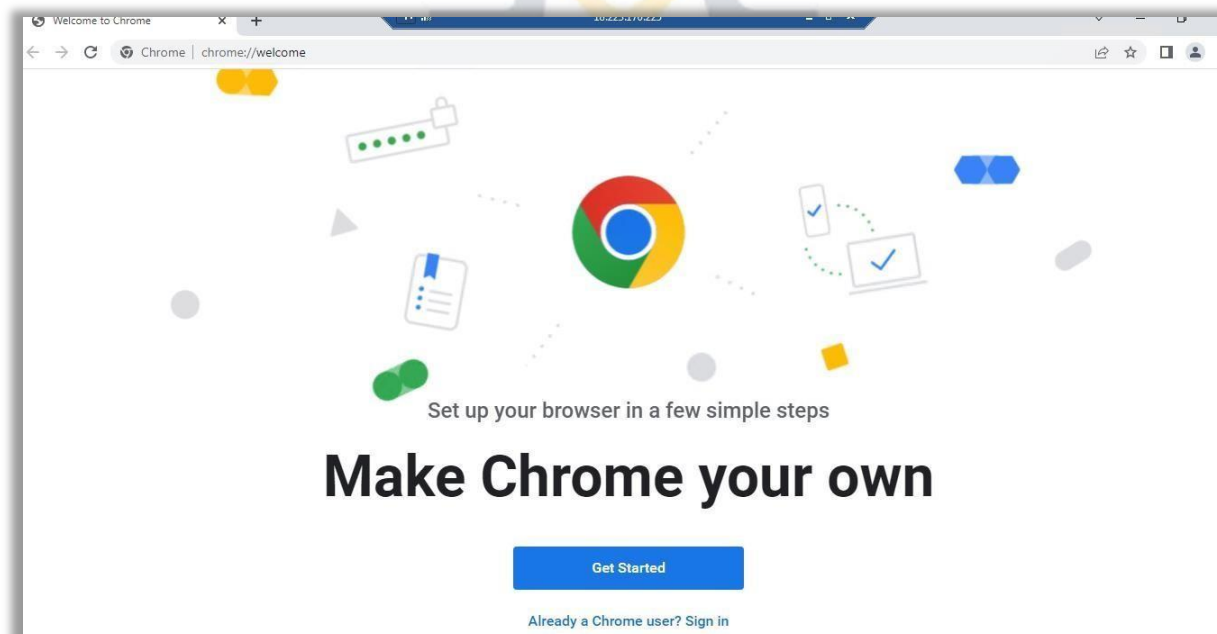
30. Come back to your Server Console



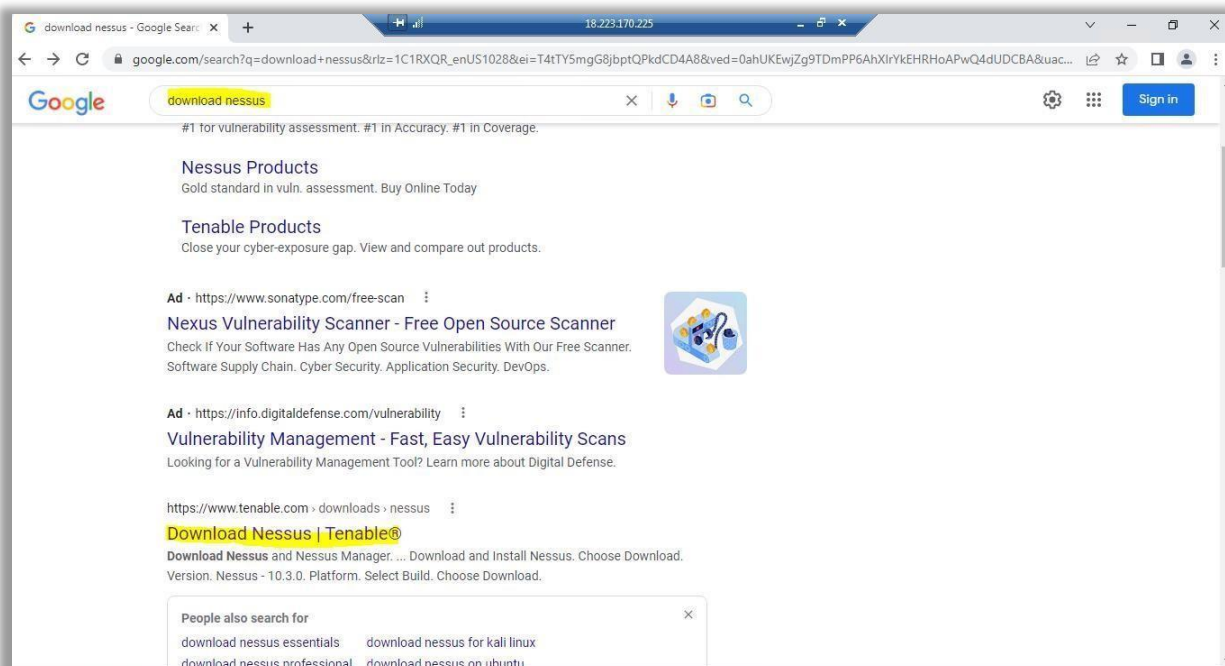
30. Then go to your Edge browser to install Chrome type in Download Chrome and Install



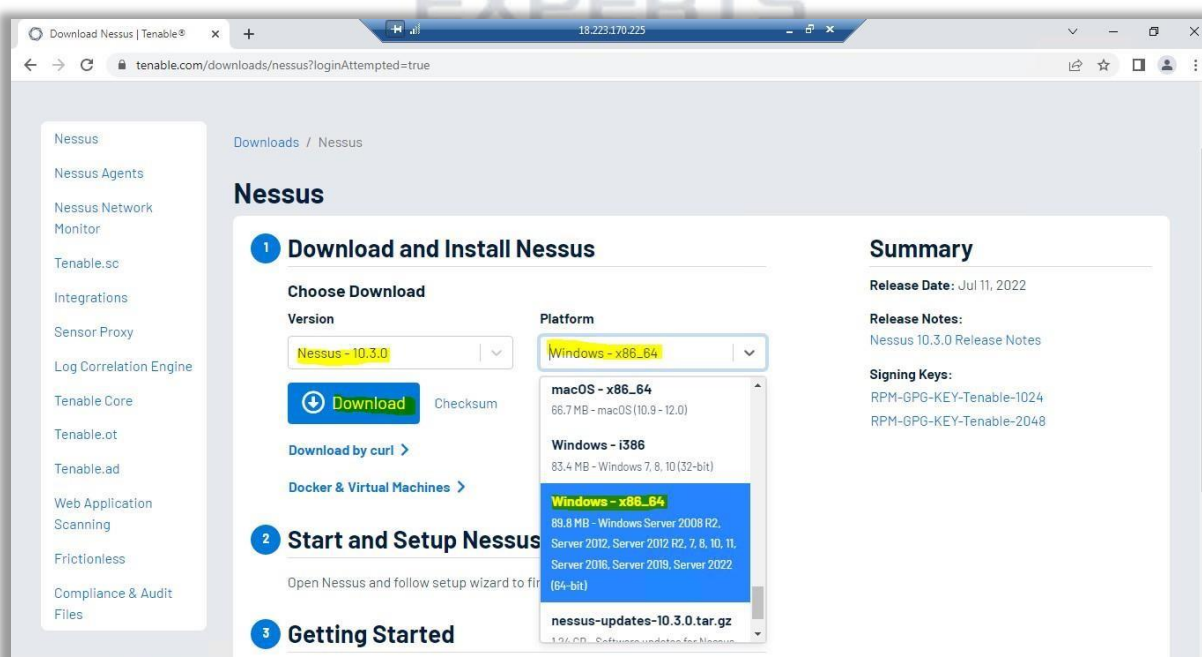
32. Install Chrome



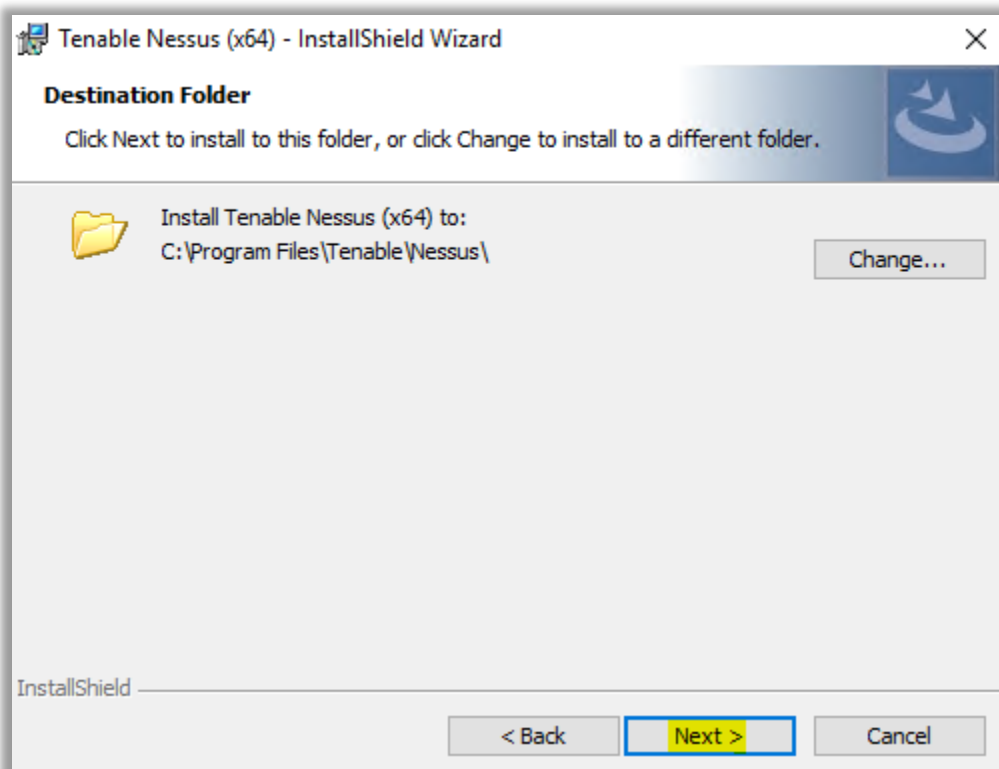
33. After Installing Chrome now we need to Download Tenable Nessus so Type inDownload Nessus in chrome search bar



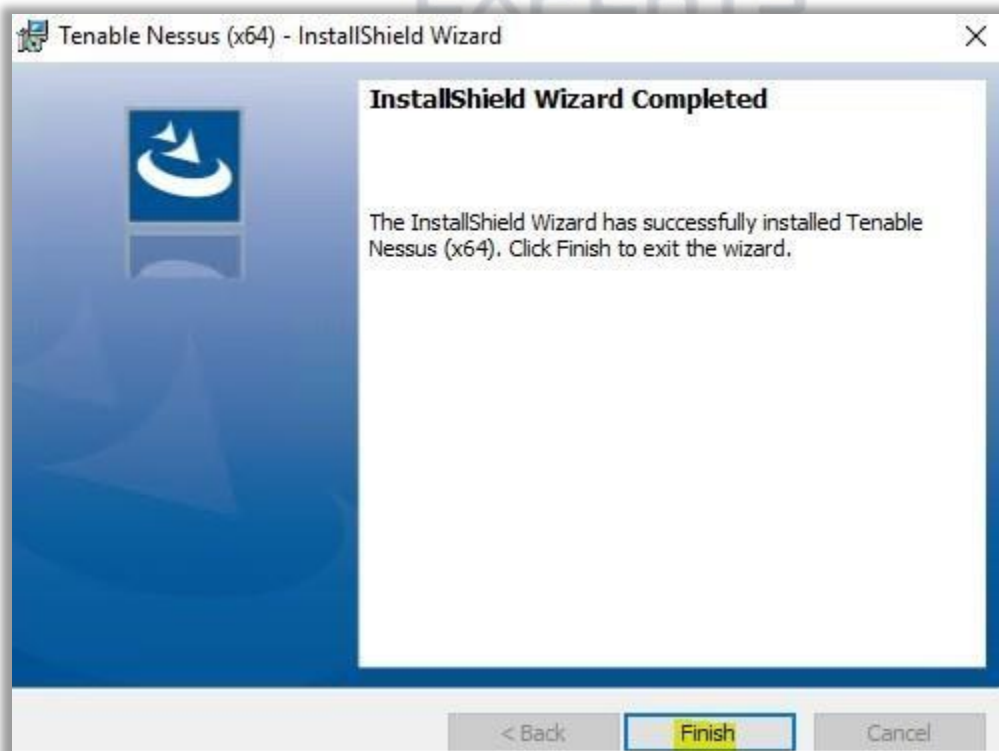
34. Sometimes by default Nessus will suggest version and platform so check for any version of Nessus and Platform should be Windows Server 2019 Base



35. The execute the downloaded file and click on Next



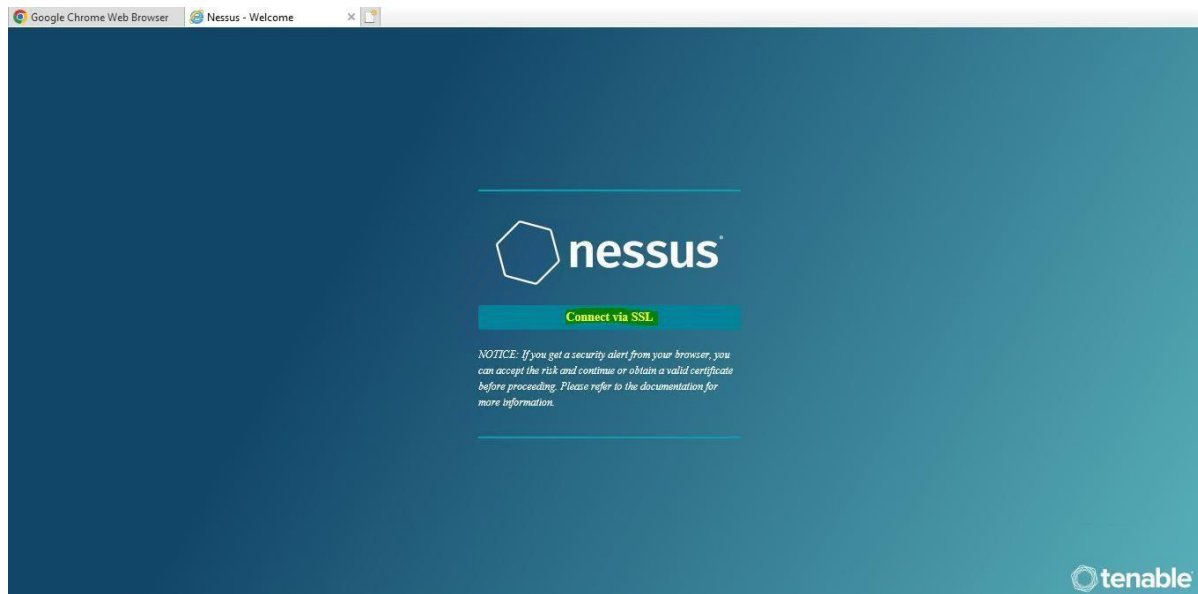
36. Click on finish to end the Installation.



Gateway to Cybersecurity Careers



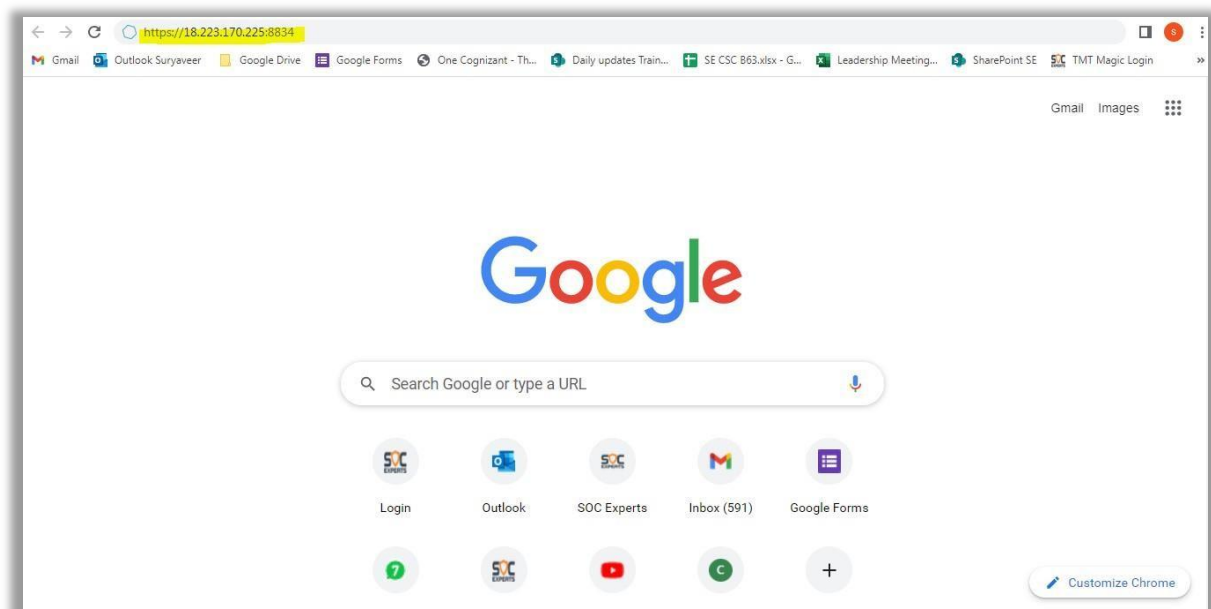
37. Then the below window will appear after 30 – 45mins of



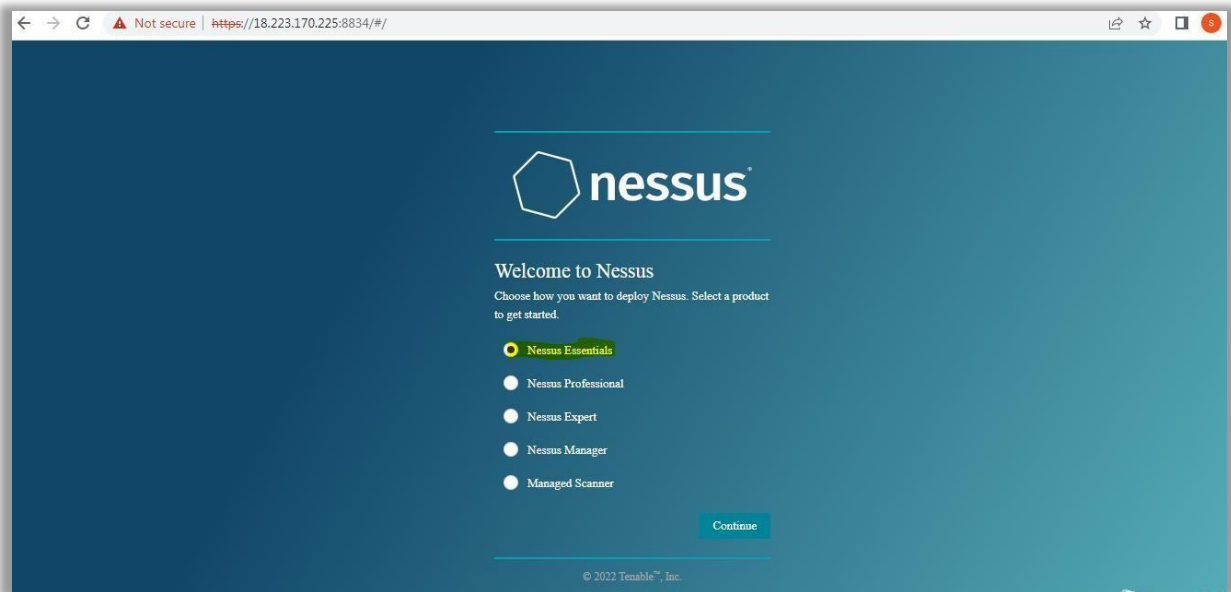
38. Now we can access the Nessus even outside the AWS as well by pasting the below url in your machines browser

Hint: Follow step No 16 to get public IP of Windows Instance.

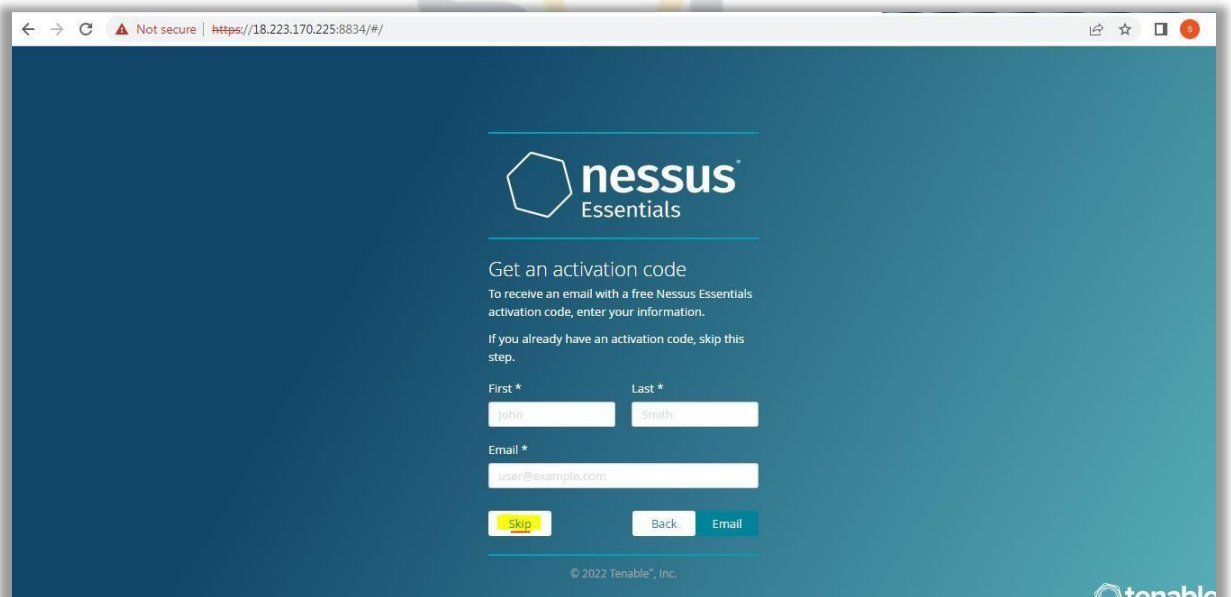
[https://paste public IP of windows instance from AWS here:8834](https://18.223.170.225:8834)



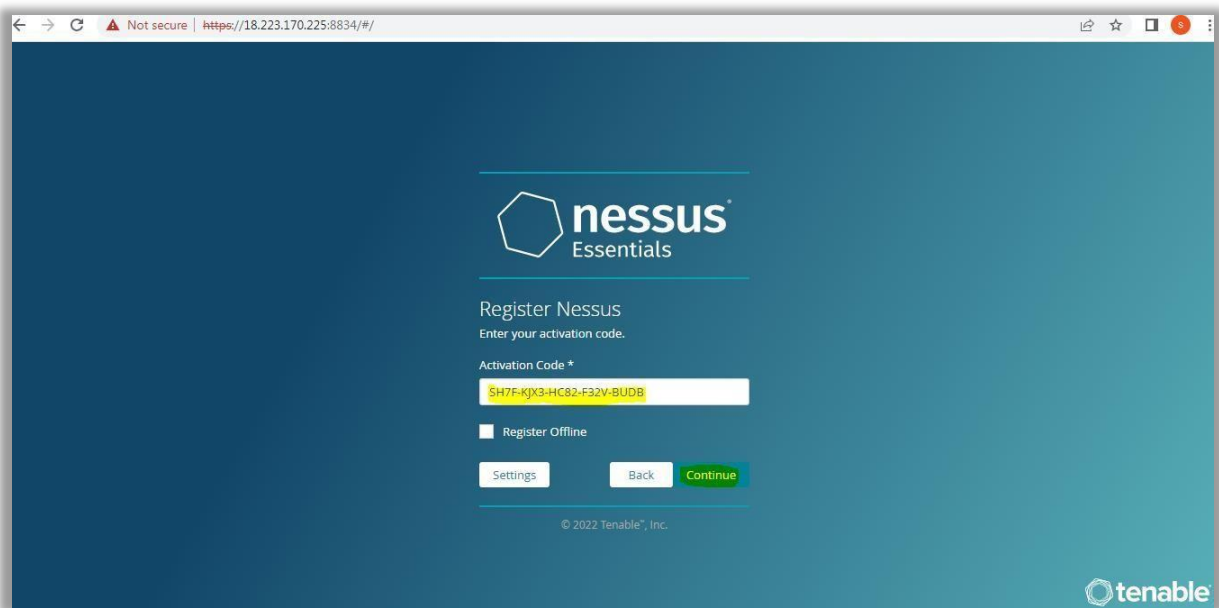
39. Once Downloading is over you should be able to see the below window and select Nessus Essentials




40. Click on Skip option as Activation code will be provided in step or else even you can sign up and get the latest code.



41. Enter the Activation Key as Below : SH7F-KJX3-HC82-F32V-BUDB



← → ↻ Not secure | https://18.223.170.225:8834/#/

 **nessus**
Essentials

Register Nessus
Enter your activation code.


Activation Code *

SH7F-KJX3-HC82-F32V-BUDB

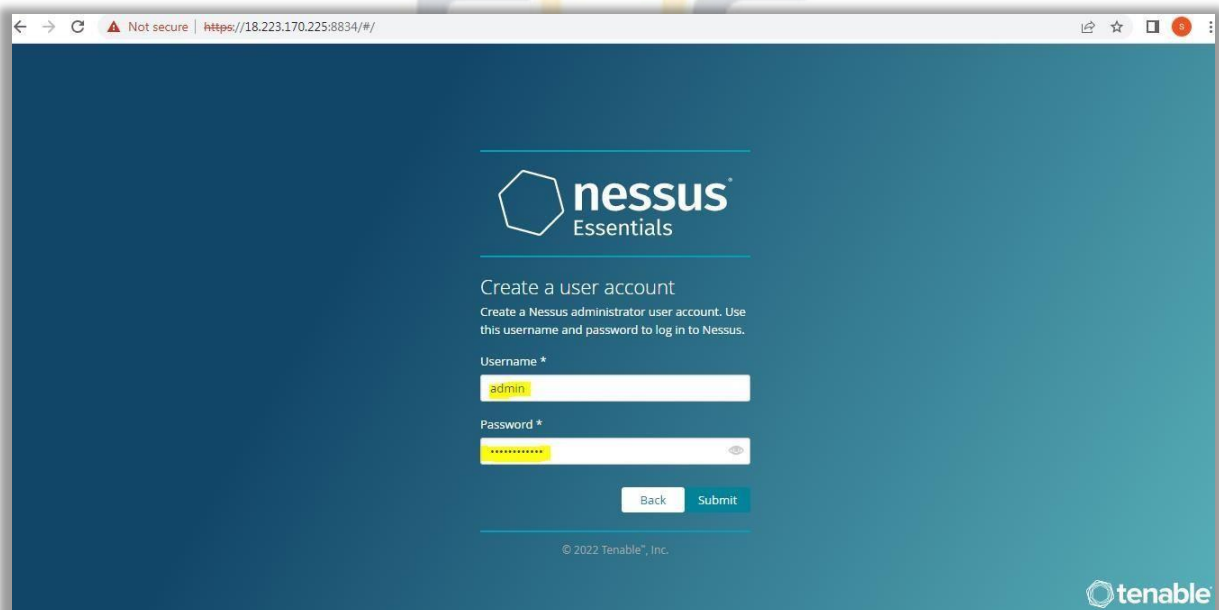
☐ Register Offline

[Settings](#) [Back](#) [Continue](#)


© 2022 Tenable®, Inc.



42. Then enter the username and password which will be used to login into your Nessus Tool



← → ↻ Not secure | https://18.223.170.225:8834/#/

 **nessus**
Essentials

Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.


Username *

admin

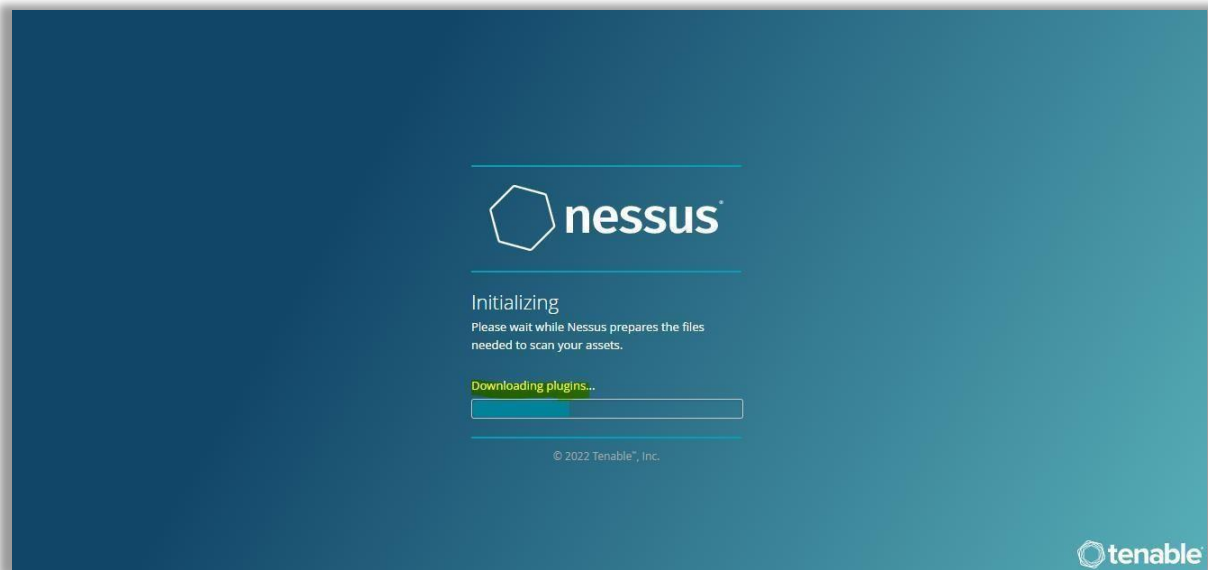
Password *

[Back](#) [Submit](#)

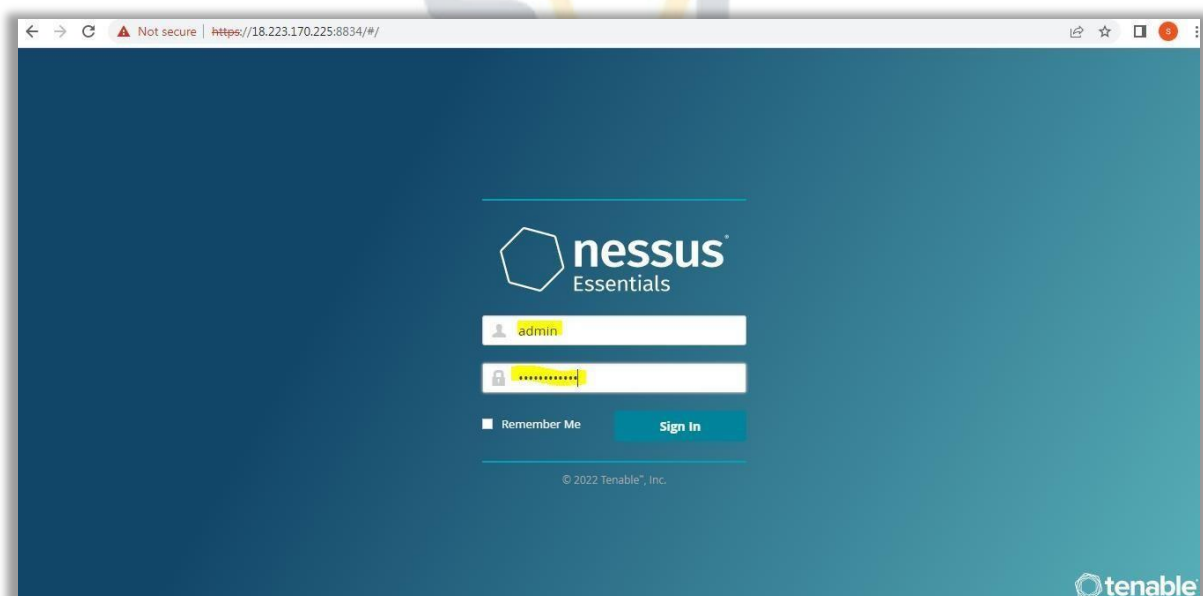
© 2022 Tenable®, Inc.



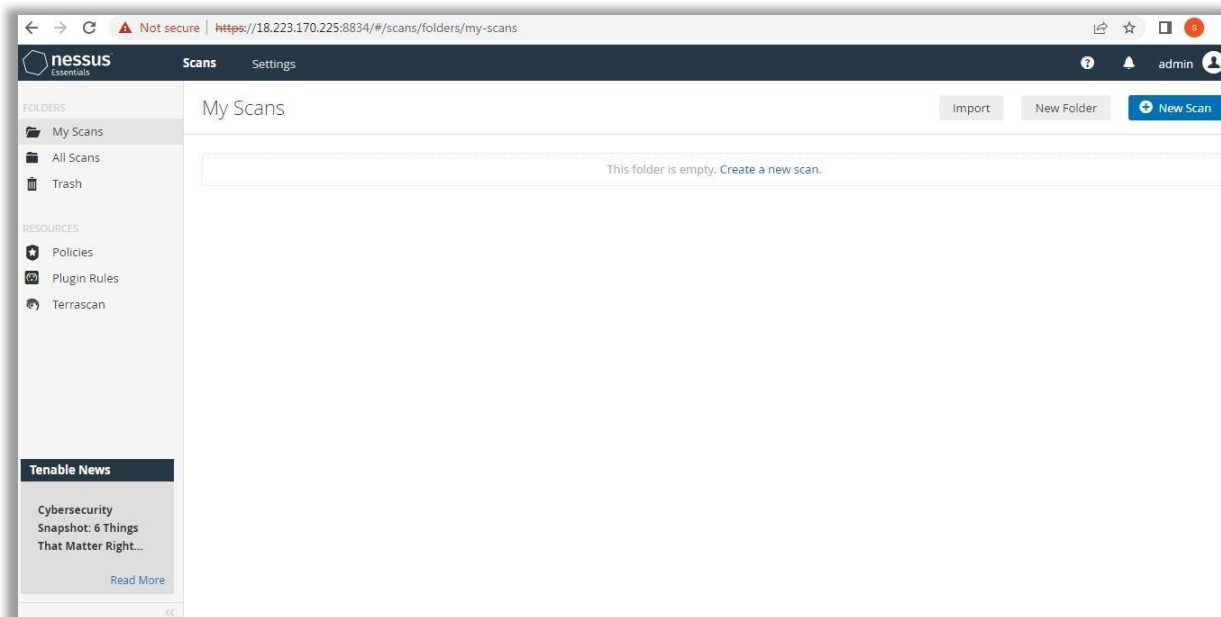
43. After successful sign up the below window may appear for 30 to 45mins so wait till all the plugins get downloaded



44. After the Plugins get downloaded enter your credentials

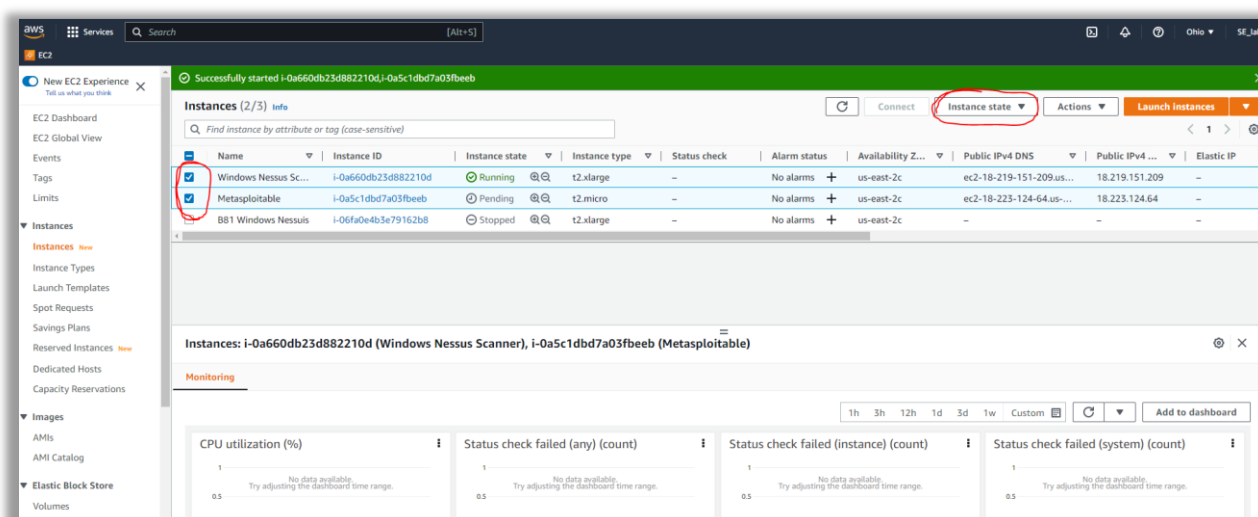


45. Hurrrrrayyyy.. Now you have completed Installation of Tenable Nessus on your AWS.

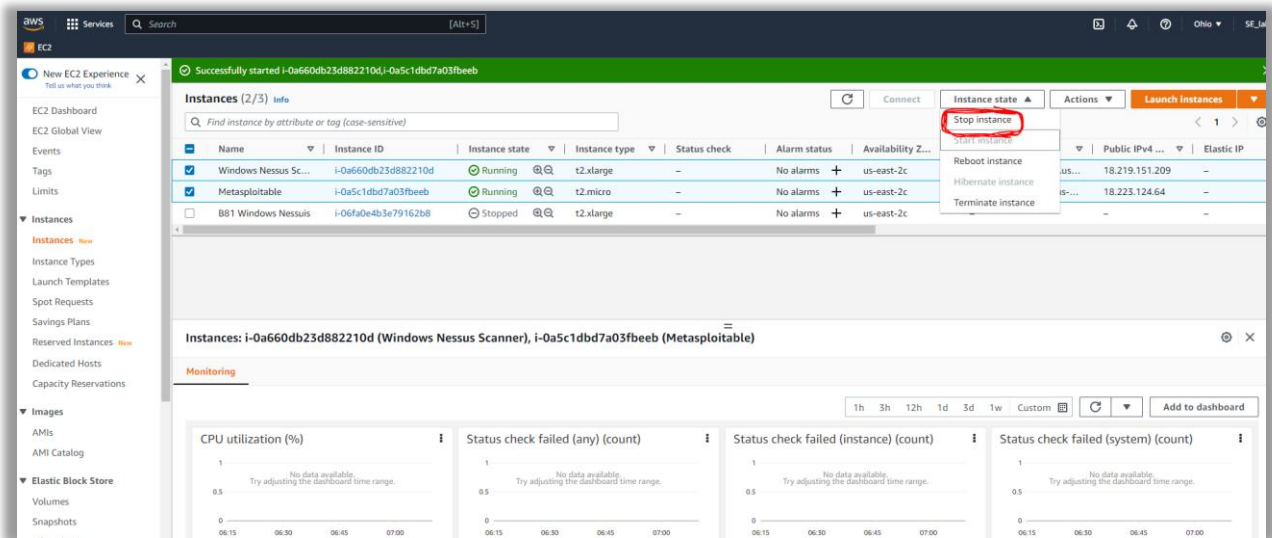


46. Once all your activity is completed in Tenable Nessus Don't Forget to Stop the Instances or else you will be charged by AWS

Select the Instances which you have spinned up and Click on Instances State Option as shown in Below Image



47. Upon completion of Step No 46 Select Stop Instances Option



The screenshot displays the AWS Management Console for the EC2 service. A green banner at the top indicates 'Successfully started i-0a660db23d882210d, i-0a5c1dbd7a03fbee'. The 'Instances (2/3)' table shows the following data:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Z...
Windows Nessus Sc...	i-0a660db23d882210d	Running	t2.xlarge	–	No alarms	us-east-2c
Metasploitable	i-0a5c1dbd7a03fbee	Running	t2.micro	–	No alarms	us-east-2c
B81 Windows Nessus	i-06fa0e4b3e79162b8	Stopped	t2.xlarge	–	No alarms	us-east-2c

The 'Instance state' dropdown menu is open, showing options: 'Stop instance' (highlighted with a red circle), 'Reboot instance', 'Hibernate instance', and 'Terminate instance'. Below the table, the 'Monitoring' section displays four graphs: 'CPU utilization (%)', 'Status check failed (any) (count)', 'Status check failed (instance) (count)', and 'Status check failed (system) (count)'. All graphs show 'No data available' for the selected time range.