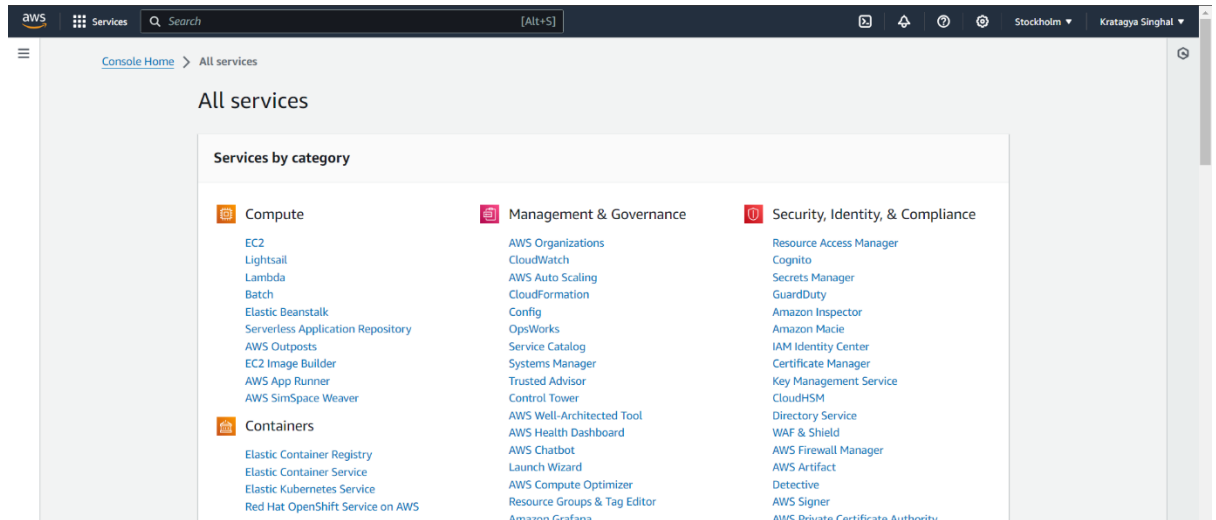
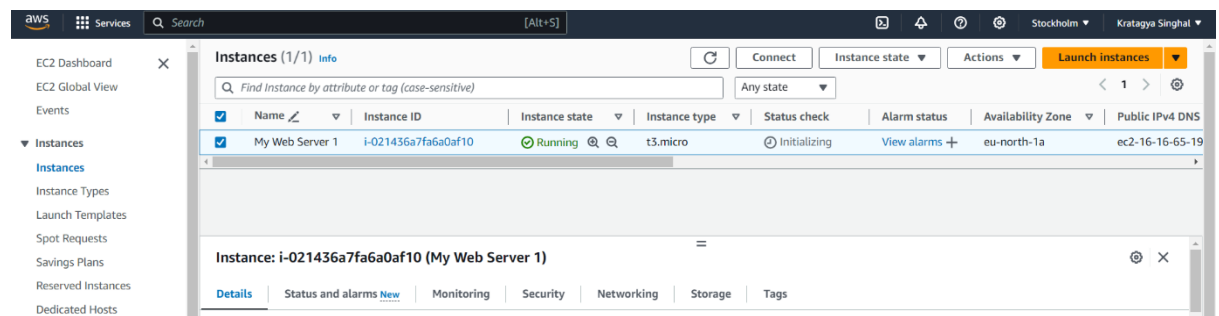


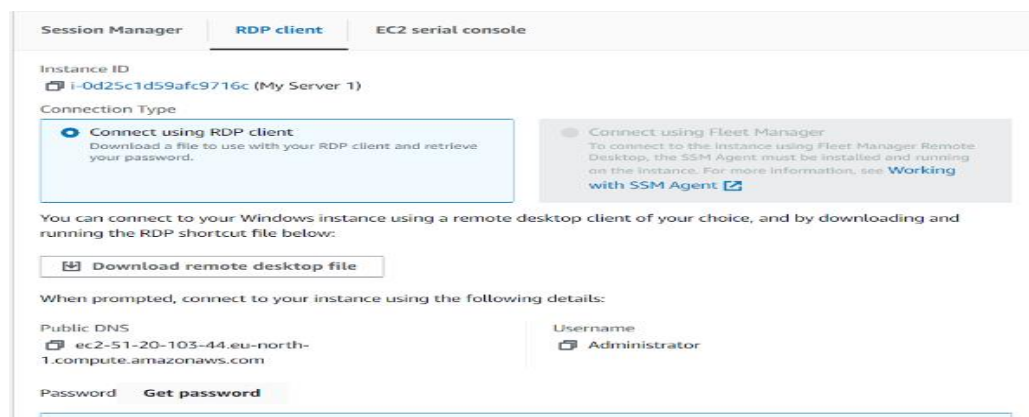
1. Sign In to your aws acc
2. Select all services
3. Select EC2



4. Launch Instance
5. Put name, create key value pair pem and save
6. Select Windows
7. Launch the instance
8. Go to instances and refresh



9. It will initialize and then start running
10. Select the instance
11. Click on connect, for connecting to RDP client



12. Click on get password and save the pass

13. Upload key value file

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

Instance ID
i-Od25c1d59afc9716c (My Server 1)

Key pair associated with this instance
Kratagya1

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

Kratagya1.pem
1.674KB

Private key contents - optional

```
-----BEGIN RSA PRIVATE KEY-----
MIIeOwIBAQAQEAhNN5wwIb8UTd/RUuwqUVawHEzcWvxJl5tMI4ExmsQN7eolZw
yMeEosNFfrX6EuaRhBKFIntZRHGUPelVrH8jhf+Agm6KYbvjRKWU9uMETuYyVou5
PaOG3kSq/vl8UVAIBFtypXHBahQb5xSLIU0fal4G68klSr8499GDfNdOHvFLmrHI
fOyQjRubGEls/oCajFDEaH8mAgOQnkD/JbsXLrcJfg2ZGKW/ZlIdaF8Jr1rUFIN4/
haOfDF4JVqUSwkDqHTGVbQC/UYdPvpEs90XgFmQ+veP7Pe7Qogglw31pYog5Q14U
eD7LKVHvgoFSZpd/hZJYojf1K213o0xd21pzwIDAQABAolBADD1I2A1es8nLxuf
n0NkTomukTe3Ud4JI874d2qy38bZxv2UECYxRDYp+4eE07P7wE8J9KtOs8yCgL2B
-----
```

14. Decrypt pass

15. Save the pass- K@yτος*0Z%coH%Va@k7KH4-\$*ggkq*Fn

Public DNS
ec2-51-20-103-44.eu-north-1.compute.amazonaws.com

Username
Administrator

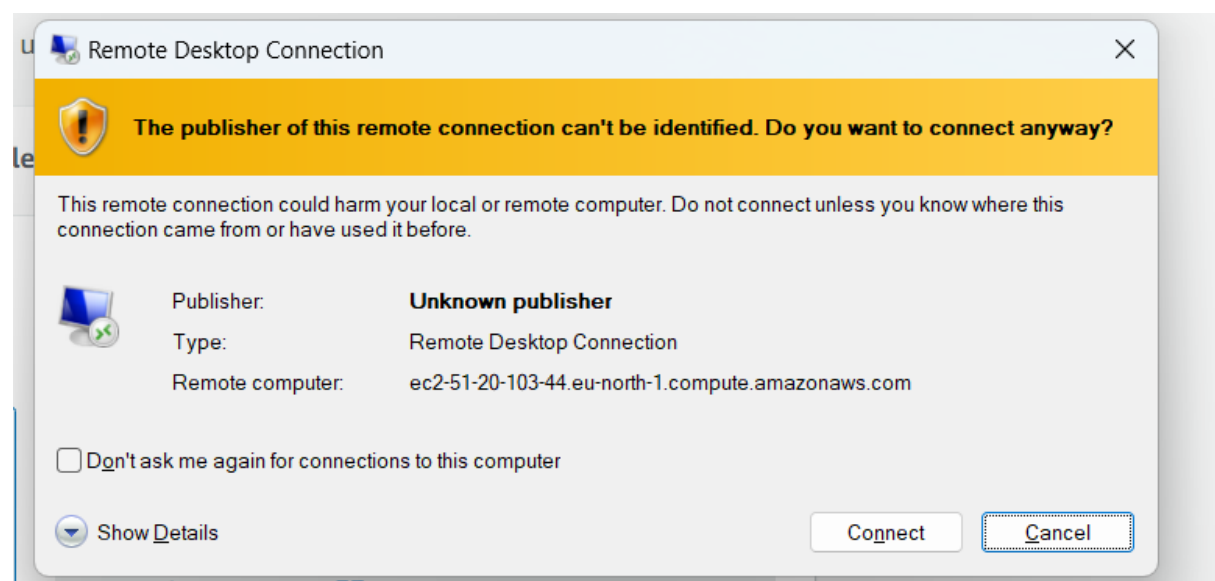
Password copied

K@yτος*0Z%coH%Va@k7KH4-\$*ggkq*Fn

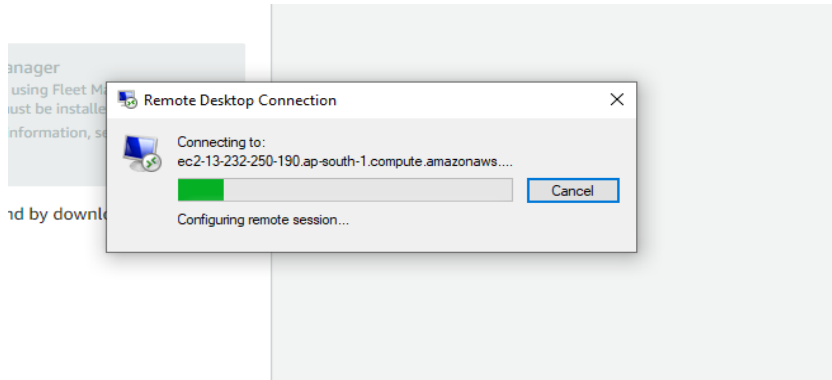
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

16. Go back to Instance, connect then download RDP file

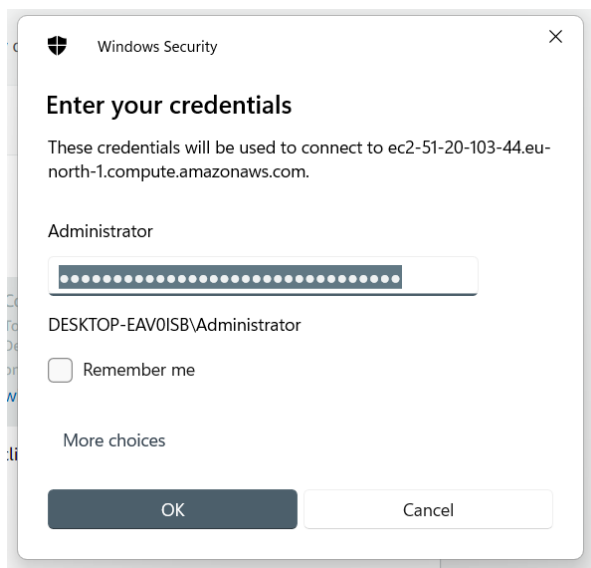
17. Open RDP



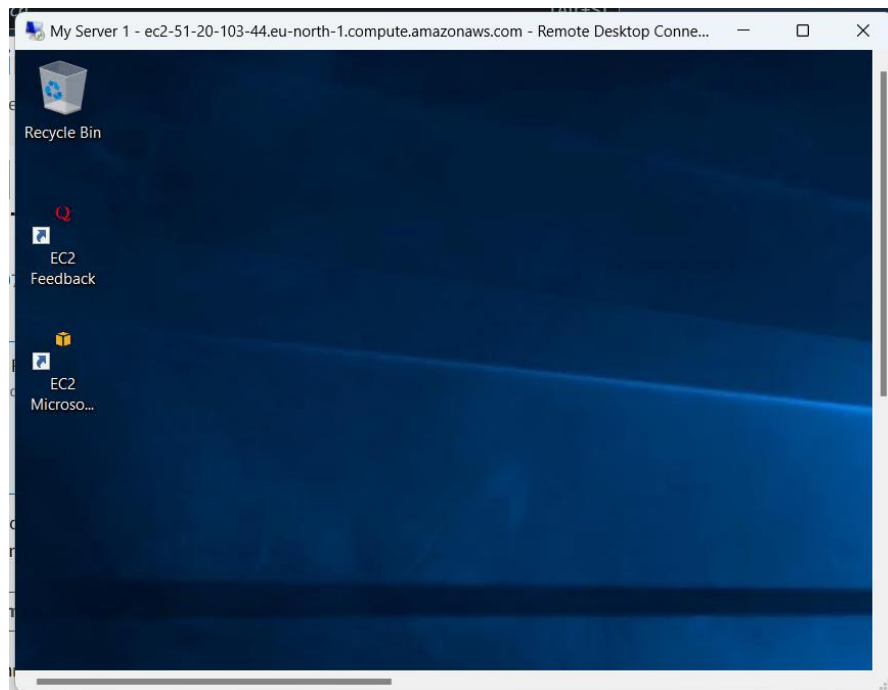
18. Connect RDP :



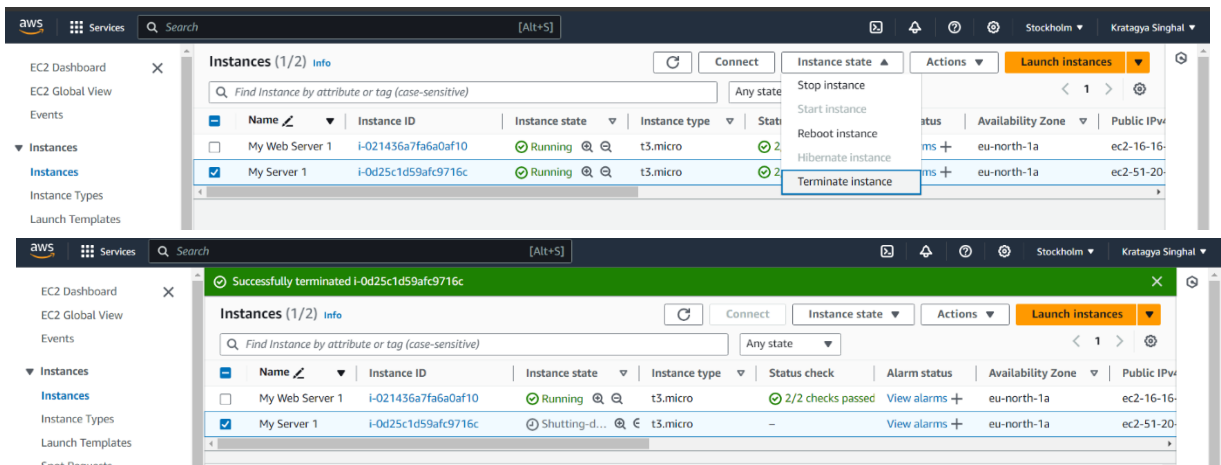
19. Enter creds



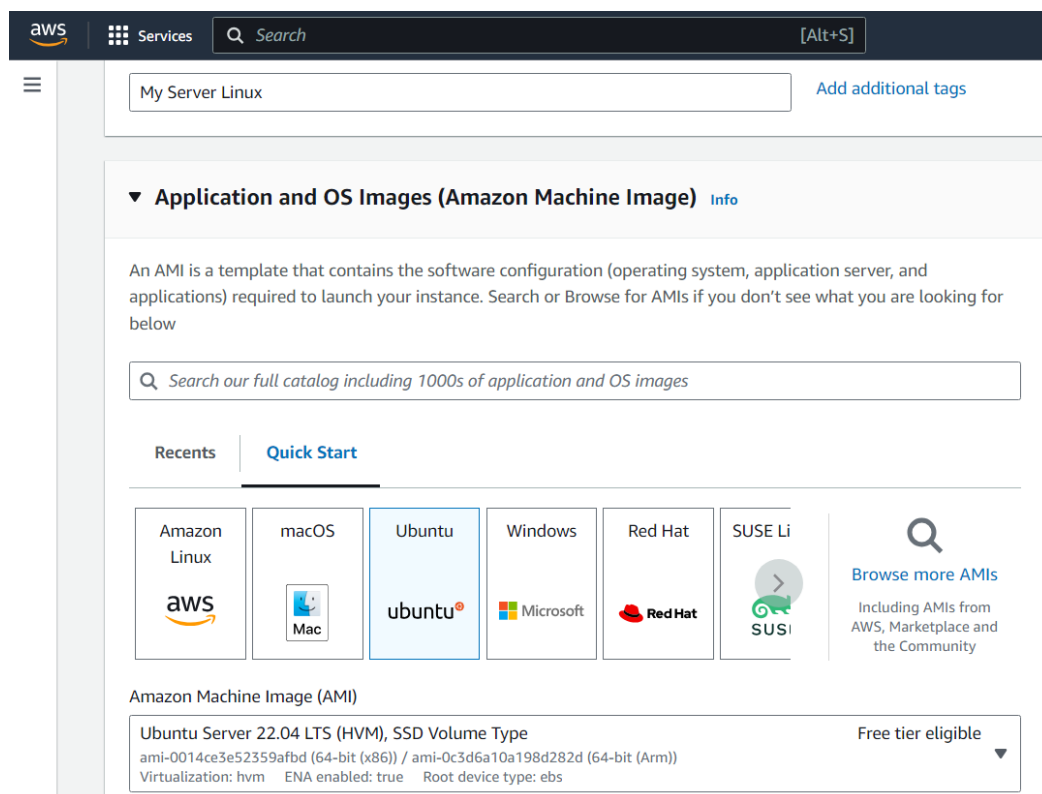
20.



21. Close RDP
22. Go back to instances
23. Terminate the instance



24. Launch a new instance for Linux:
25. Write a new web server name and Select Ubuntu server



26. Create a new key value pair and select ppk

The screenshot shows the 'Create key pair' dialog box. It has a title bar 'Create key pair' with a close button. Below the title bar, there is a section 'Key pair name' with a text input field and a note: 'Key pairs allow you to connect to your instance securely. The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.' Below this is a section 'Key pair type' with two radio buttons: 'RSA' (selected) and 'ED25519'. Below that is a section 'Private key file format' with two radio buttons: '.pem' and '.ppk' (selected). At the bottom, there is a yellow warning box with a triangle icon and text: 'When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more'. At the very bottom are 'Cancel' and 'Create key pair' buttons.

27. Download putty.exe from google

28. Select and download exe file

Package files

You probably want one of these. They include versions of all the PuTTY utilities (except the new and slightly experimental Windows pterr
(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge download at the [Microsoft Store](#); they usually

MSI ('Windows Installer')

64-bit x86:	putty-64bit-0.80-installer.msi	(signature)
64-bit Arm:	putty-arm64-0.80-installer.msi	(signature)
32-bit x86:	putty-0.80-installer.msi	(signature)

Unix source archive

.tar.gz:	putty-0.80.tar.gz	(signature)
----------	-----------------------------------	-------------

29. Create ppk key value pair and save the file

30. Allow all traffic

Network settings [Info](#) [Edit](#)

Network [Info](#)
vpc-04a9c583cef010d37

Subnet [Info](#)
No preference (Default subnet in any availability zone)

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

We'll create a new security group called 'launch-wizard-2' with the following rules:

- ☒ Allow SSH traffic from Helps you connect to your instance Anywhere (0.0.0.0/0)
- ☒ Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server
- ☒ Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

⚠ 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. ✕

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...re
ami-03f4878755434977f

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year 750 hours of t2.micro (or t2.xlarge) in the Regions in which t2.micro is available. Instance usage tier AMIs per month, 30 GiB storage, 2 million I/Os, 1 GB snapshots, and 100 GB of traffic to the internet.

Cancel [Launch](#)

31. Launch Instance

32. Go to Instances and refresh

33. Select and copy Public IPV4 address

Instances (1/3) [Info](#) [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find Instance by attribute or tag (case-sensitive) [Any state](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
My Web Server 1	i-021436a7fa6a0af10	Running	t3.micro	2/2 checks passed	View alarms +	eu-north-1a	ec2-16-
My Server Linux	i-01b7254269a62f269	Running	t3.micro	Initializing	View alarms +	eu-north-1a	ec2-51-
My Server 1	i-0d25c1d59afc9716c	Terminated	t3.micro	-	View alarms +	eu-north-1a	-

Instance: i-01b7254269a62f269 (My Server Linux)

Instance ID: i-01b7254269a62f269 (My Server Linux)

Private IPv4 addresses: 172.31.31.198

Public IPv4 DNS: ec2-51-20-71-159.eu-north-1.compute.amazonaws.com [Open address](#)

34. Go to putty, paste IP address

PuTTY Configuration

Category:

- Session
- Logging
- Terminal
- Keyboard
- Bell
- Features
- Window
- Appearance
- Behaviour
- Translation
- Selection
- Colours
- Connection
- Data
- Proxy
- SSH
- Serial
- Telnet
- Rlogin
- SUPDUP

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

Connection type: ☒ SSH ☐ Serial ☐ Other: Telnet

Load, save or delete a stored session

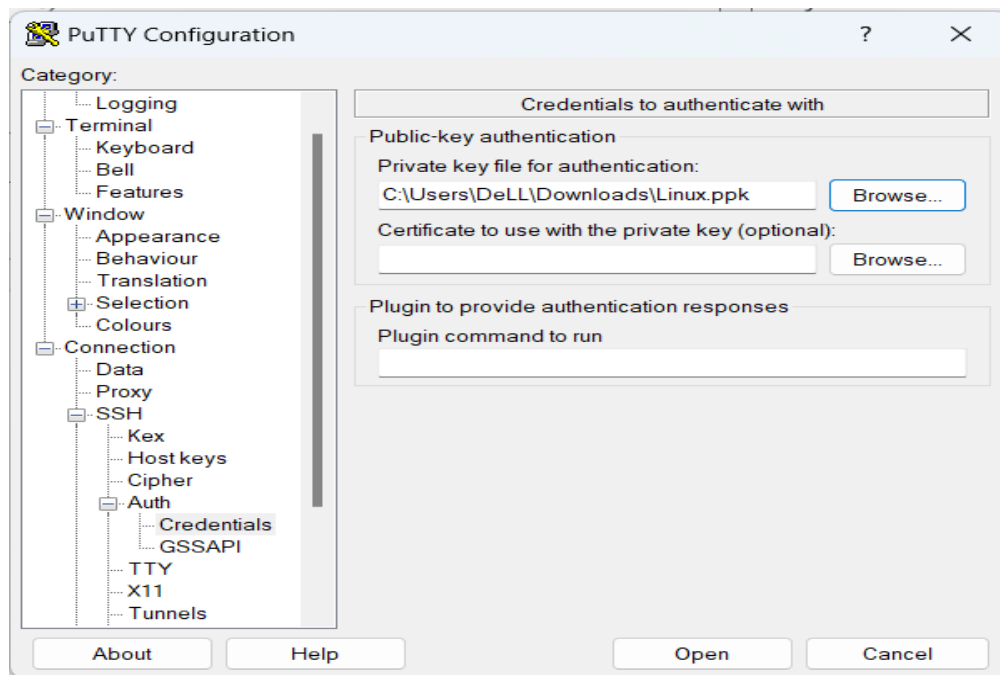
Saved Sessions

Default Settings [Load](#) [Save](#) [Delete](#)

Close window on exit: ☐ Always ☐ Never ☒ Only on clean exit

[About](#) [Help](#) [Open](#) [Cancel](#)

35. Category -> SSH -> Auth -> Credentials -> Browse and select ppk file



36. Putty will launch

37. Login as Ubuntu

```
ubuntu@ip-172-31-31-198: ~  
login as: ubuntu  
Authenticating with public key "Linux"  
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Mon Jan 29 14:58:44 UTC 2024  
  
System load:  0.0           Processes:            99  
Usage of /:   20.5% of 7.57GB Users logged in:       0  
Memory usage: 21%          IPv4 address for ens5: 172.31.31.198  
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.
```

38. Type commands-

mkdir – Makes a directory

ls- lists down the files and folders in the directory

Control + D - Used to exit the file when inside Cat

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

```
ubuntu@ip-172-31-31-198:~$ mkdir My Server Linux  
ubuntu@ip-172-31-31-198:~$ ls  
Linux My Server  
ubuntu@ip-172-31-31-198:~$ cd My Server Linux
```

control + D

39. Type exit command to exit putty

40. Go back to instances in AWS and select the current instance

41. TO TERMINATE THE CURRENT RUNNING INSTANCE:

Instances -> Select Instance -> Instance state -> Terminate the Instance

The screenshot displays the AWS Management Console interface for EC2 instances. The top navigation bar includes the AWS logo, 'Services' menu, a search bar, and user information (Stockholm, Kratagya Singhal). The left sidebar shows the 'Instances' menu selected. The main content area, titled 'Instances (1/3) Info', contains a table of instances. The instance 'My Server Linux' (ID: i-01b7254269a62f269) is selected. A context menu is open over this instance, showing options like 'Stop instance', 'Start instance', 'Reboot instance', 'Hibernate instance', and 'Terminate instance'. The 'Terminate instance' option is highlighted. Below the table, a green banner indicates 'Successfully terminated i-01b7254269a62f269'. The table below the banner shows the instance's state as 'Shutting-down' and 'Initializing'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
My Web Server 1	i-021436a7fa6a0af10	Running	t3.micro	2/2 checks passed	View alarms +	eu-north-1a	ec2-16-
My Server Linux	i-01b7254269a62f269	Shutting-down	t3.micro	Initializing	View alarms +	eu-north-1a	ec2-51-
My Server 1	i-0d25c1d59afc9716c	Terminated	t3.micro	-	View alarms +	eu-north-1a	-