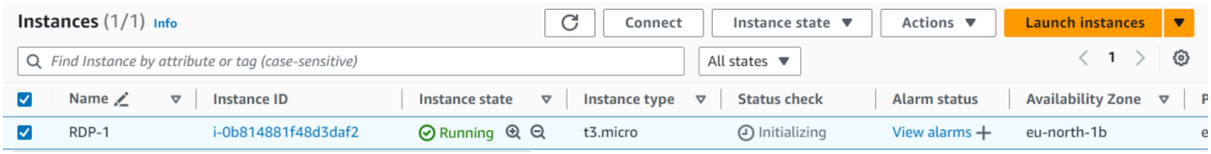
LAB -6: *RDP CLIENT [WINDOWS]:*

AIM: Is to connect to a **WINDOWS** client with the help of RDP in AWS.

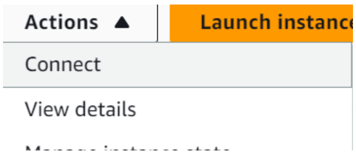
1. Open the Amazon EC2 console.



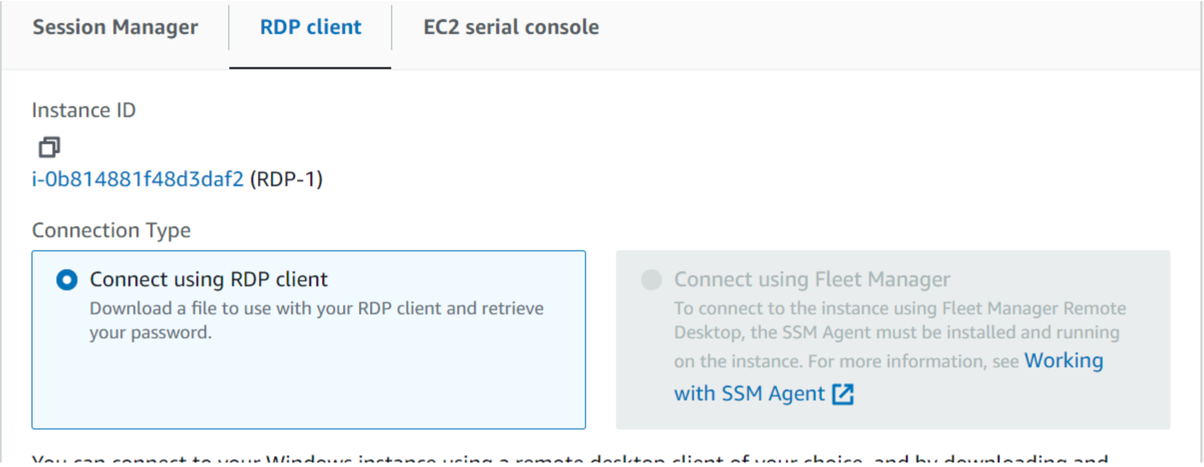
☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	P
☑	RDP-1	i-0b814881f48d3daf2	Running	t3.micro	Initializing	View alarms +	eu-north-1b	e

2. From the navigation pane, choose **Instances**.

3. Select the instance and then choose **Connect**.



4. On the **Connect to instance** page, choose the **RDP client** tab.



Instance ID

i-0b814881f48d3daf2 (RDP-1)

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

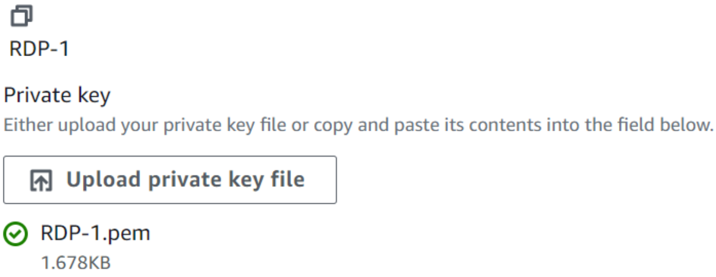
5. For **Username**, choose the default username for the Administrator account. The username you choose must match the language of the operating system (OS) contained in the AMI that you used to launch your instance. If there is no username in the same language as your OS, choose **Administrator (Other)**.
6. Choose **Get password**.

7. On the **Get Windows password** page, do the following:

a. Choose **Upload private key file** and navigate to the private key (.pem) file that you specified when you launched the instance. Select the file and choose **Open** to copy the entire contents of the file to this window.

b. Choose **Decrypt password**. The **Get Windows password** page closes, and the default administrator password for the instance appears under **Password**, replacing the **Get password** link shown previously.

c. Copy the password and save it in a safe place. This password is required to connect to the instance.



RDP-1

Private key

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

RDP-1.pem

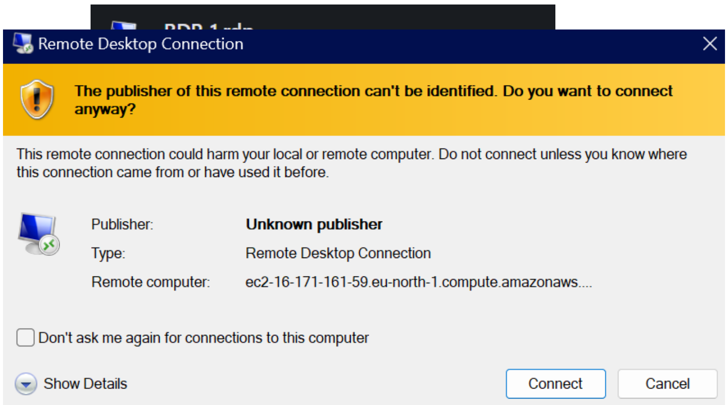
1.678KB

8. Choose **Download remote desktop file**. Your browser prompts you to either open or save the RDP shortcut file. When you have finished downloading the file, choose **Cancel** to return to the **Instances** page.

    1. If you opened the RDP file, you'll see the **Remote Desktop Connection** dialog box.

    2. If you saved the RDP file, navigate to your downloads directory, and open the RDP file to display the dialog box.

9. You might get a warning that the publisher of the remote connection is unknown. Choose **Connect** to continue to connect to your instance.



Remote Desktop Connection

The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher: **Unknown publisher**

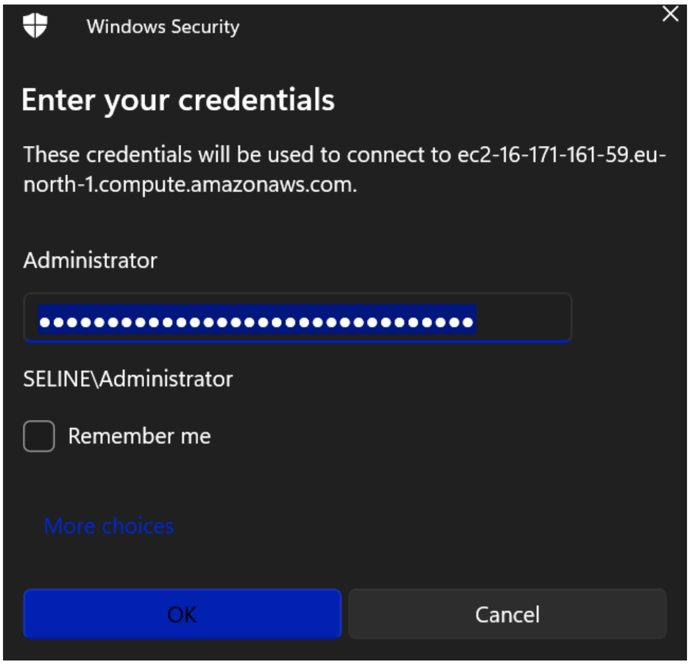
Type: Remote Desktop Connection

Remote computer: ec2-16-171-161-59.eu-north-1.compute.amazonaws....

□ Don't ask me again for connections to this computer

10.Choose **Yes** when asked if we want to connect despite certificate errors.

11.Enter the **password** you have saved earlier.



Windows Security

Enter your credentials

These credentials will be used to connect to ec2-16-171-161-59.eu-north-1.compute.amazonaws.com.

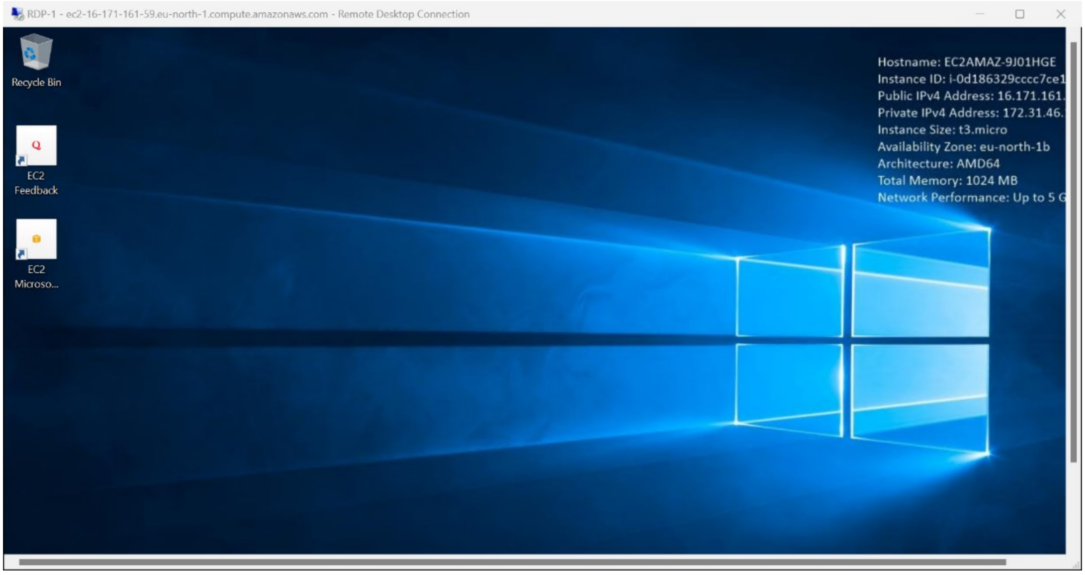
Administrator

•••••••••••••••••••••••••••••••••

SELINE\Administrator

□ Remember me

12. Youre windows desktop is connected through RDP client



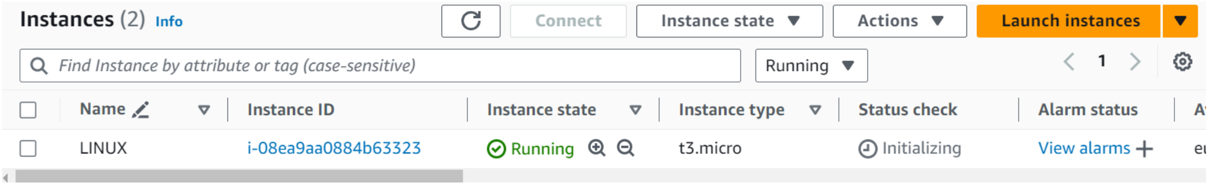
RDP-1 - ec2-16-171-161-59.eu-north-1.compute.amazonaws.com - Remote Desktop Connection

Hostname: EC2AMAZ-9J01HGE
Instance ID: i-0d186329cccc7ce1
Public IPv4 Address: 16.171.161.
Private IPv4 Address: 172.31.46.
Instance Size: t3.micro
Availability Zone: eu-north-1b
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Up to 5 G

LAB -7: *CONNECT TO CLIENT USING PuTTY:*

AIM: Is to connect to a **LINUX [CLIENT]** using PuTTY and PuTTY GEN.

1. Create instances with Ubuntu platform and .pem key pair.

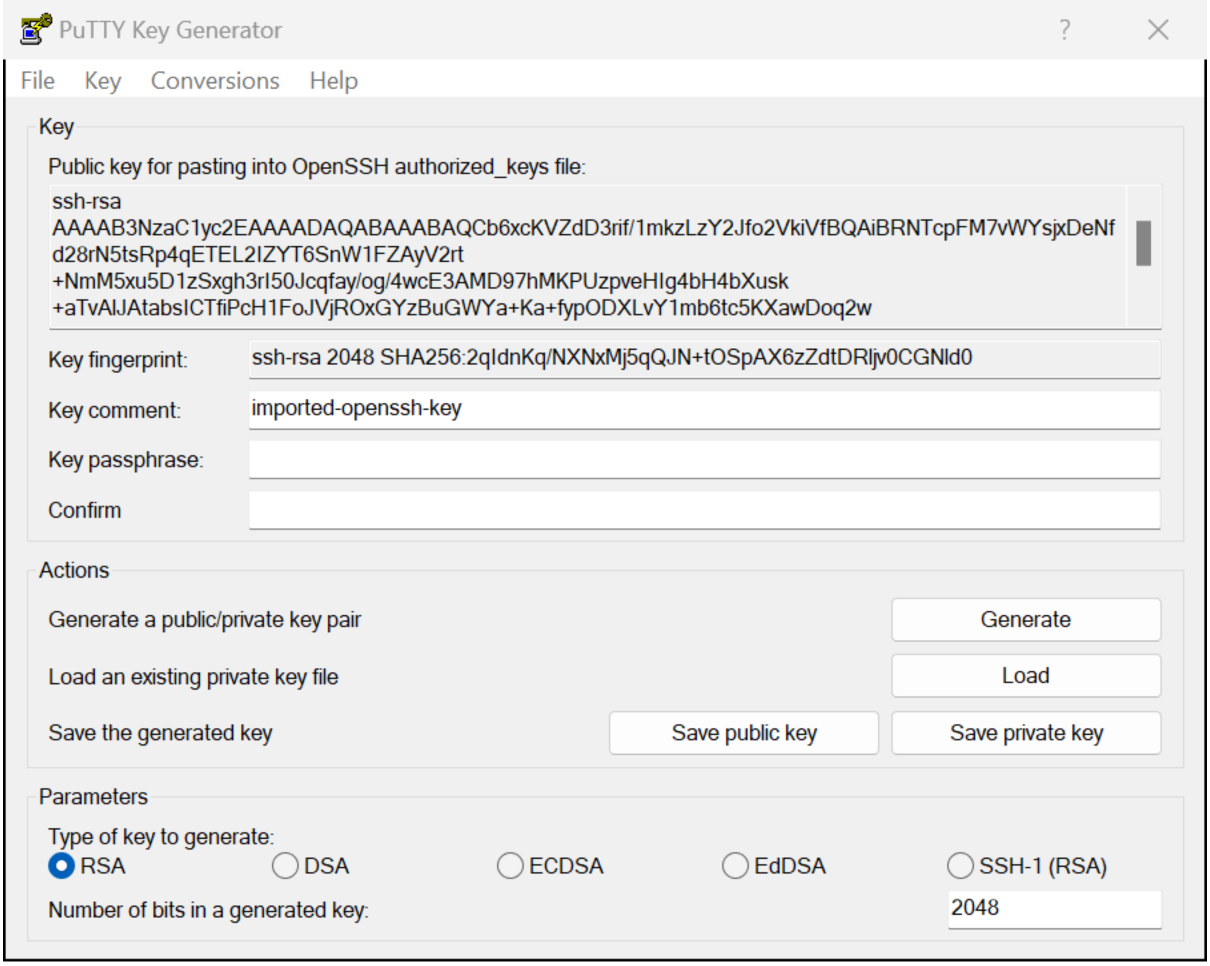


Instances (2) Info

Find Instance by attribute or tag (case-sensitive) | Running

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	A
☐	LINUX	i-08ea9aa0884b63323	✓ Running	t3.micro	Initializing	View alarms +	e

2. In PuTTY GEN, open the .pem file and **Save private Key**.



PuTTY Key Generator

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCb6xcKVZdD3rif/1mkzLzY2Jfo2VkiVfBQAiBRNTcpFM7vWYsjxDeNf
d28rN5tsRp4qETEL2IZYT6SnW1FZAyV2rt
+NmM5xu5D1zSxgh3rI50Jcqfay/og/4wcE3AMD97hMKPUzpveHIg4bH4bXusk
+aTvAlJAtabsICTfiPcH1FoJVjROxGYzBuGWYa+Ka+fypODXLvY1mb6tc5KXawDoq2w
```

Key fingerprint: ssh-rsa 2048 SHA256:2qIdnKq/NXNxMj5qQJN+tOSpAX6zZdtDRljv0CGNld0

Key comment: imported-openssh-key

Key passphrase:

Confirm

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate:

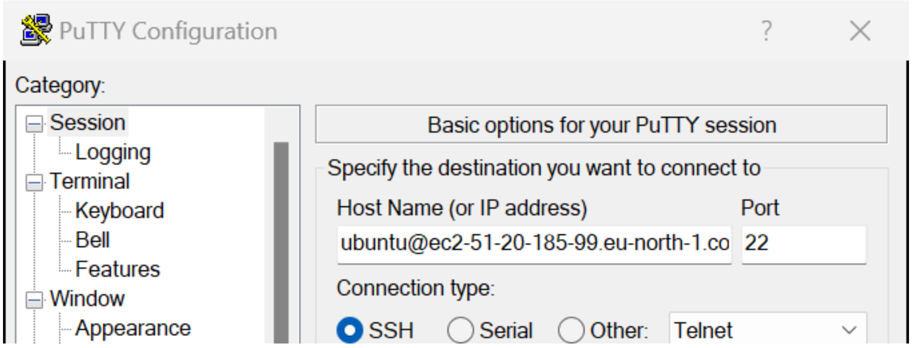
● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

3. Open PuTTY and select **Session** and in **Host Name** do **enter**

instance-user-name@instance-public-dns-name.

Here, instance username is ubuntu



Basic options for your PuTTY session

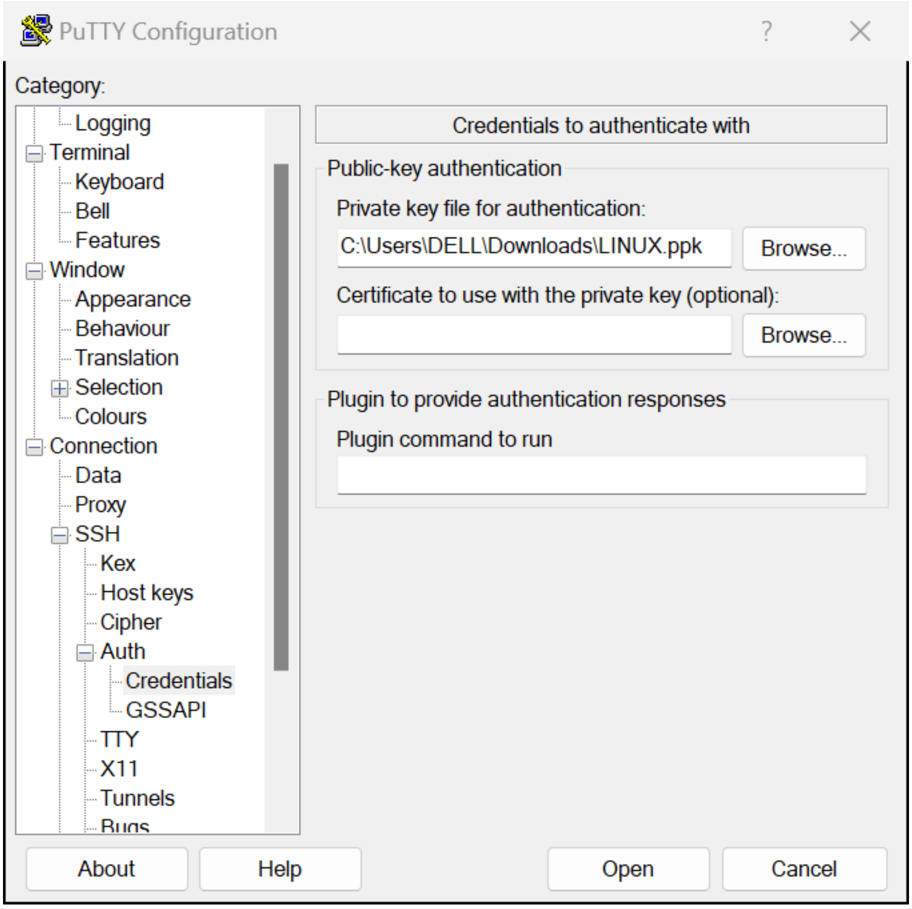
Specify the destination you want to connect to

Host Name (or IP address): ubuntu@ec2-51-20-185-99.eu-north-1.co

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

4. Go to **CONNECTIONS – SSH – Auth** and in **Private key file for authentication, open the .ppk file you have downloaded**



Credentials to authenticate with

Public-key authentication

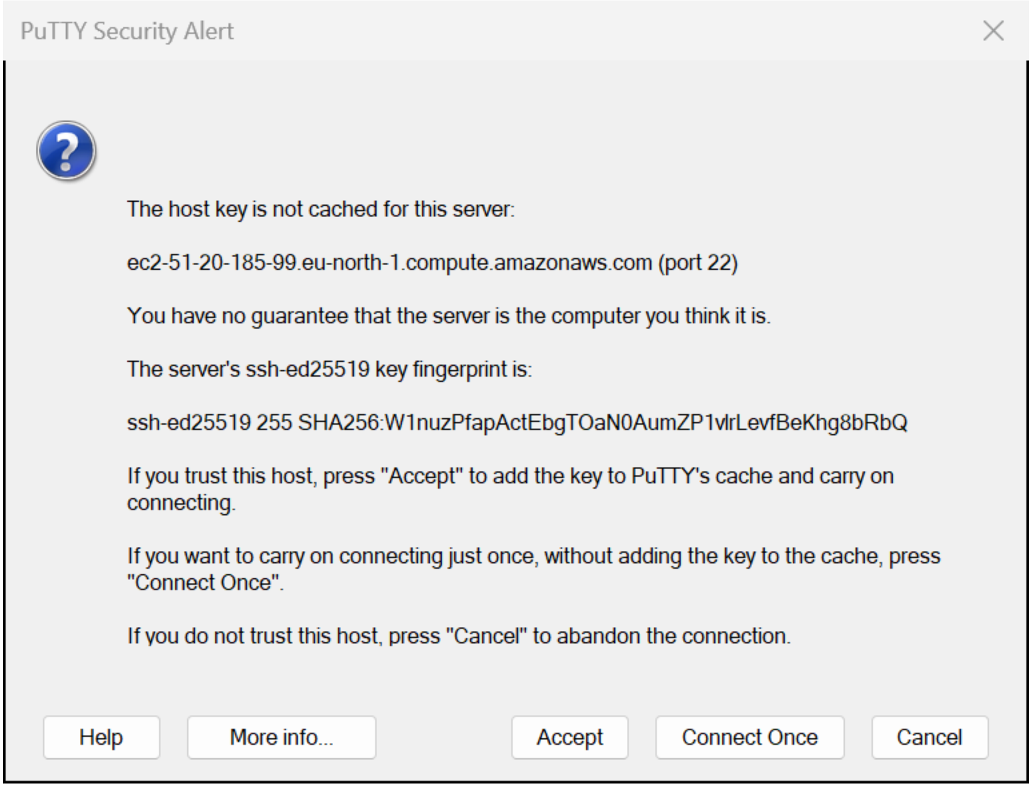
Private key file for authentication: C:\Users\DELL\Downloads\LINUX.ppk [Browse...]

Certificate to use with the private key (optional): [Browse...]

Plugin to provide authentication responses

Plugin command to run

5. Click on **Open.**



The host key is not cached for this server:

ec2-51-20-185-99.eu-north-1.compute.amazonaws.com (port 22)

You have no guarantee that the server is the computer you think it is.

The server's ssh-ed25519 key fingerprint is:

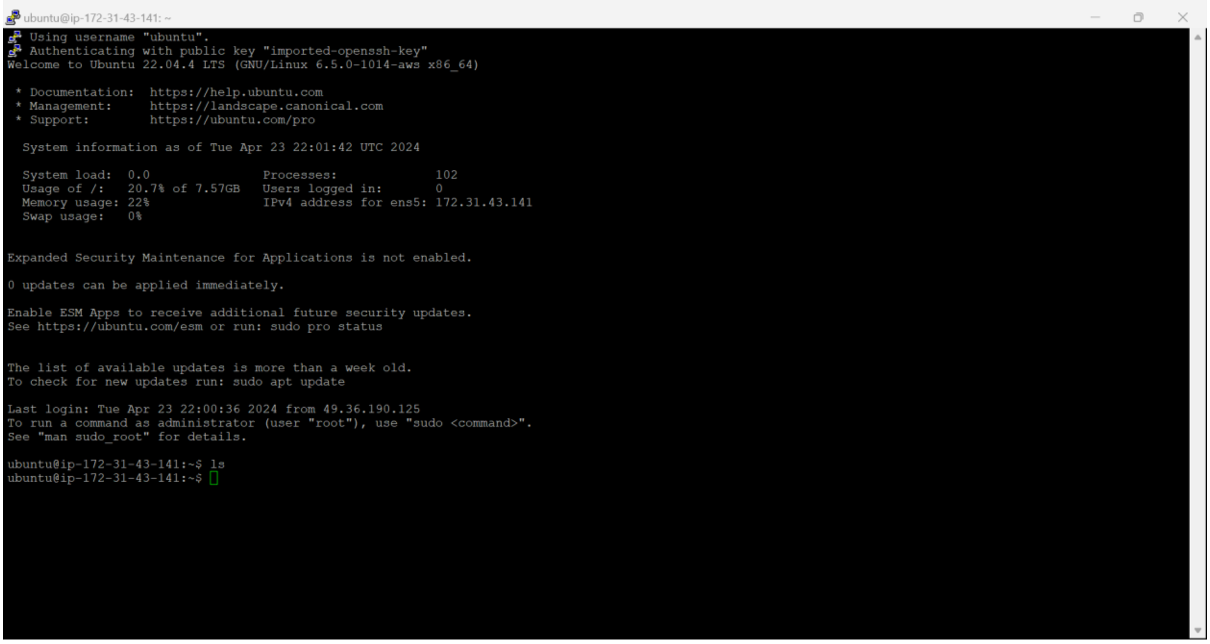
ssh-ed25519 255 SHA256:W1nuzPfapActEbgTOaN0AumZP1vlrLevfBeKhg8bRbQ

If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".

If you do not trust this host, press "Cancel" to abandon the connection.

6. Click on **Accept/ Connect Once.**



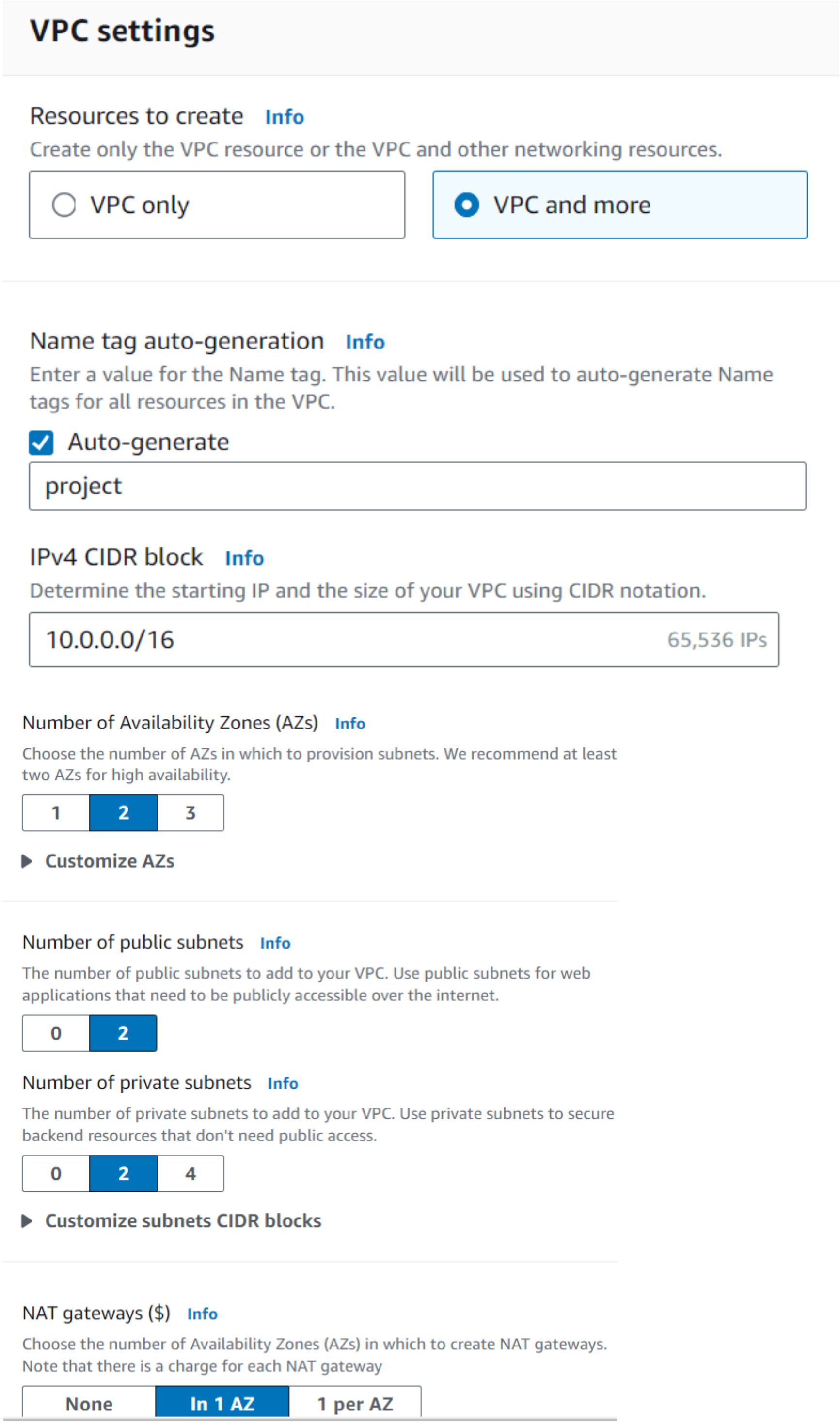
```
Using username "ubuntu".
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1014-aws x86_64)

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

  System information as of Tue Apr 23 22:01:42 UTC 2024

  System load:  0.0               Processes:             102
  Usage of /:   20.7% of 7.57GB   Users logged in:       0
  Memory usage: 22%               IPv4 address for ens5: 172.31.43.141
  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

Last login: Tue Apr 23 22:00:36 2024 from 49.36.190.125
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-43-141:~$ ls
ubuntu@ip-172-31-43-141:~$ 
```

7. Your client has started running.

LAB 8: *NAT:*

AIM: Is to connect to a **NAT INSTANCE**.

1. Create VPC for NAT Instance



VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

○ VPC only   ● VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

project

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16   65,536 IPs

Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 [✓ 2] 3

▶ Customize AZs

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 [✓ 2]

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 [✓ 2] 4

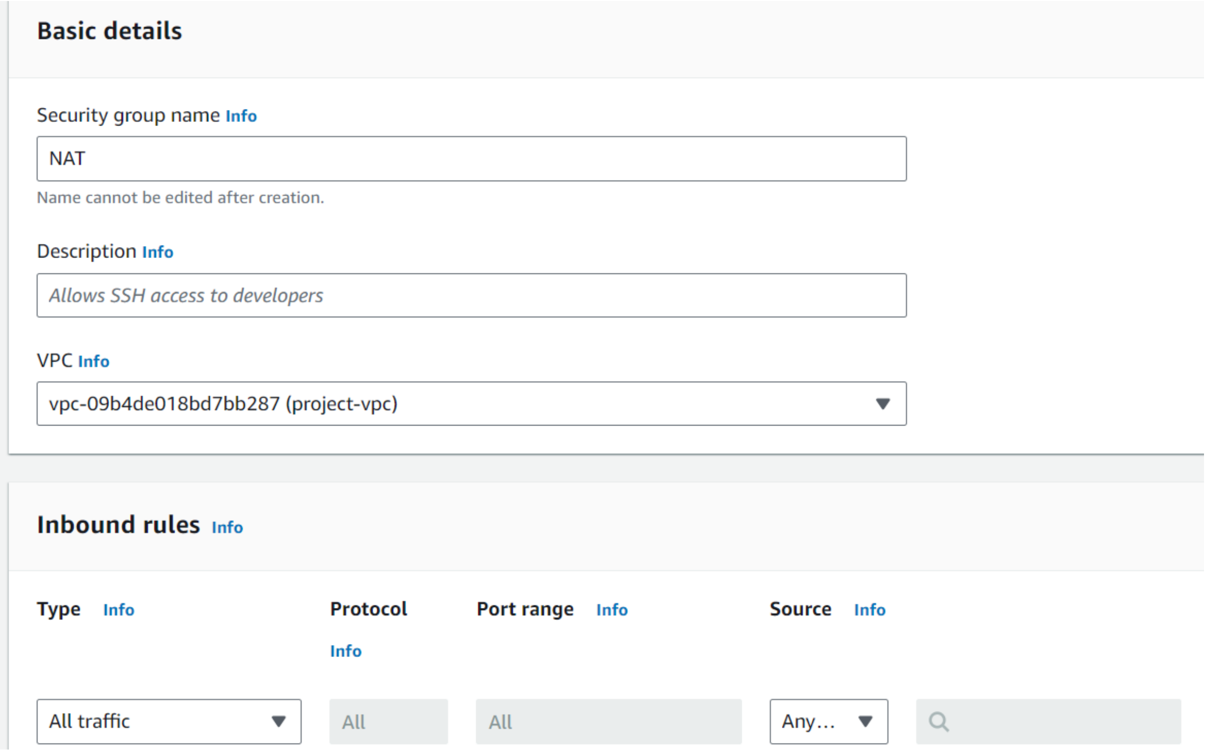
▶ Customize subnets CIDR blocks

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None [✓ In 1 AZ] 1 per AZ

2. Create security groups



Basic details

Security group name Info

NAT

Name cannot be edited after creation.

Description Info

Allows SSH access to developers

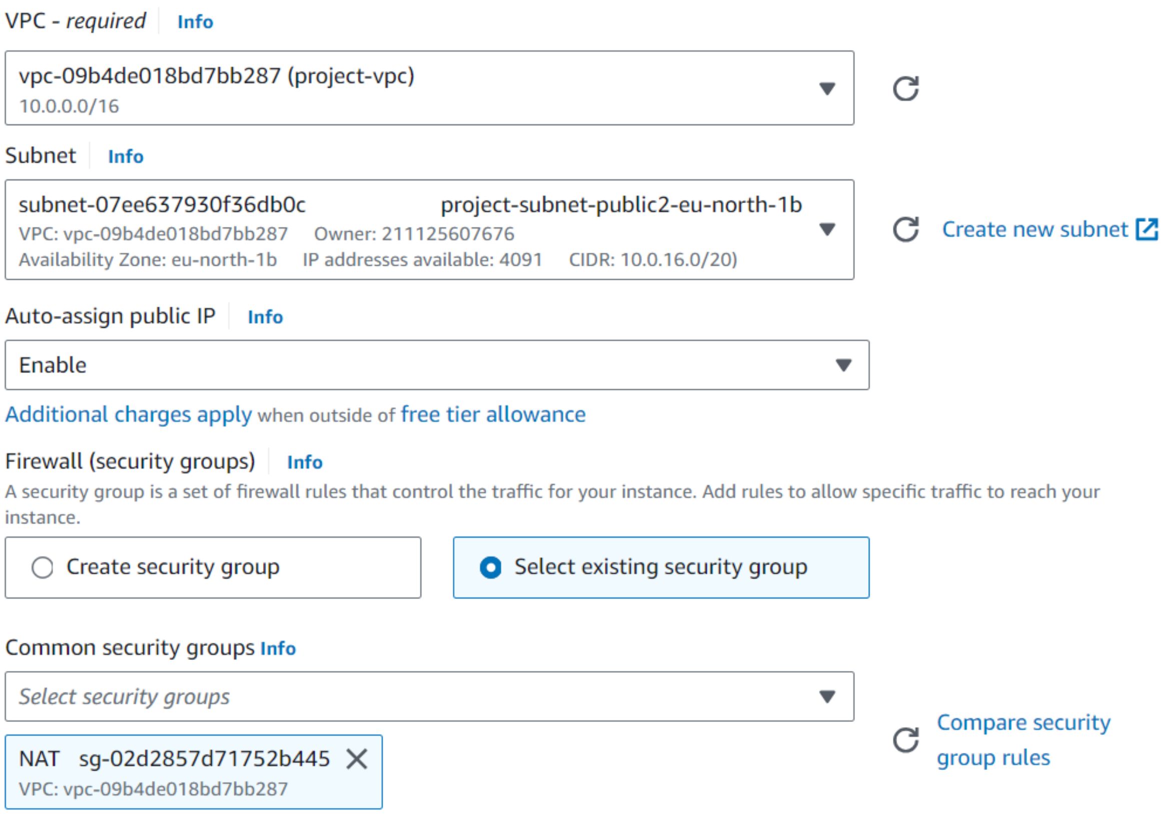
VPC Info

vpc-09b4de018bd7bb287 (project-vpc) ▼

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info	
All traffic ▼	All	All	Any… ▼	🔍

3. Launch an Instance with the following details



VPC - *required* Info

vpc-09b4de018bd7bb287 (project-vpc) ▼
10.0.0.0/16

Subnet Info

subnet-07ee637930f36db0c project-subnet-public2-eu-north-1b ▼
VPC: vpc-09b4de018bd7bb287 Owner: 211125607676
Availability Zone: eu-north-1b IP addresses available: 4091 CIDR: 10.0.16.0/20)

Auto-assign public IP Info

Enable ▼

Additional charges apply when outside of free tier allowance

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.

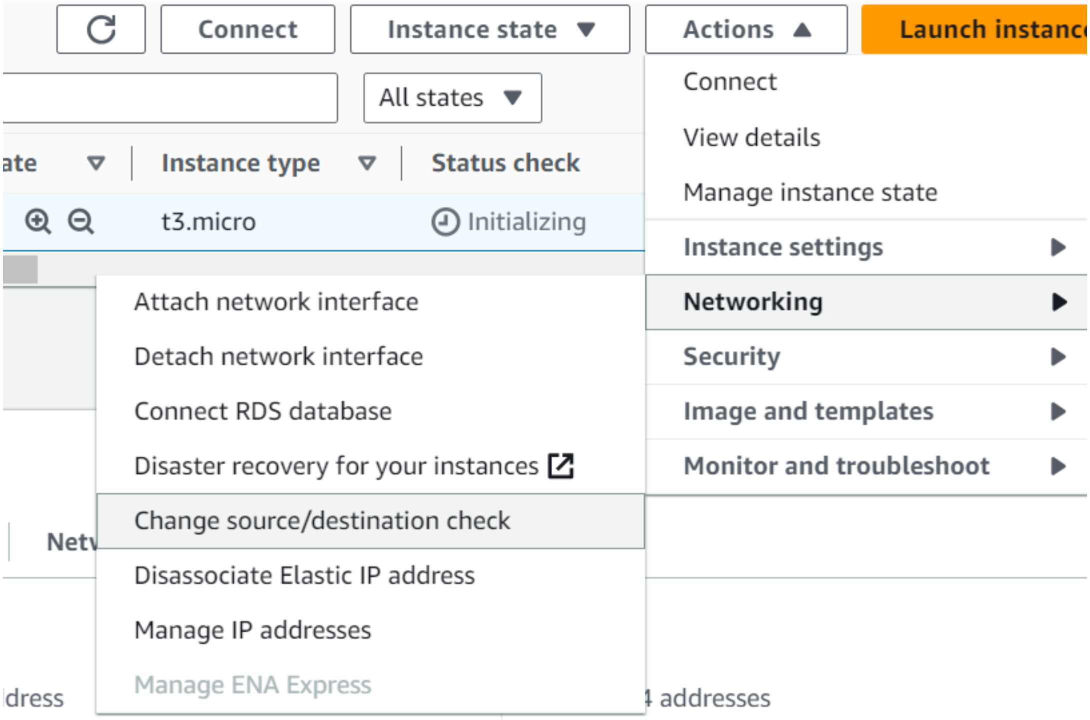
○ Create security group ● Select existing security group

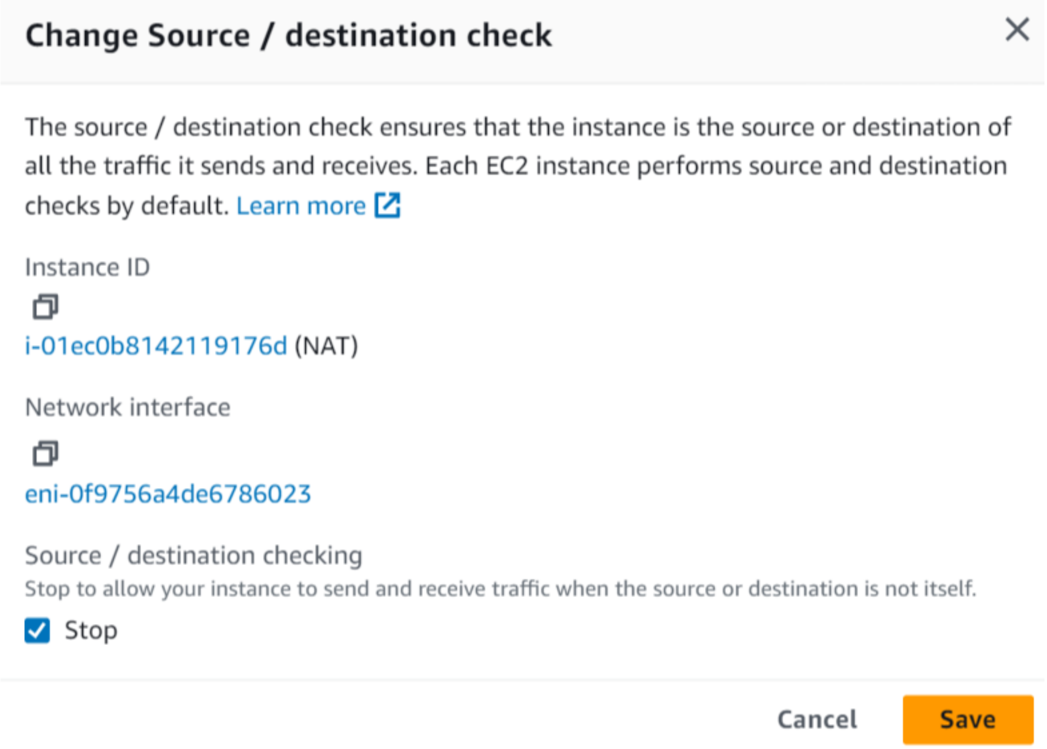
Common security groups Info

Select security groups ▼

NAT sg-02d2857d71752b445 ✕
VPC: vpc-09b4de018bd7bb287

4. Select the instance and click on NETWORKING – CHANGE SOURCE/DESTINATION CHECK.





Change Source / destination check

The source / destination check ensures that the instance is the source or destination of all the traffic it sends and receives. Each EC2 instance performs source and destination checks by default. Learn more

Instance ID

i-01ec0b8142119176d (NAT)

Network interface

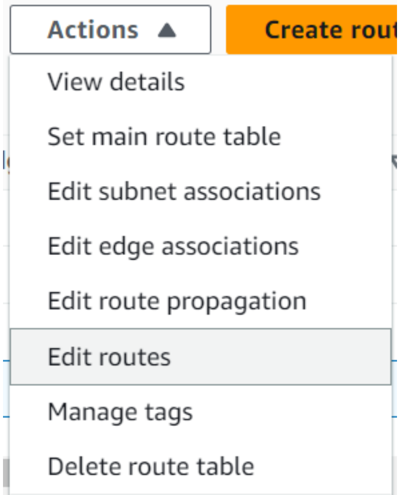
eni-0f9756a4de6786023

Source / destination checking

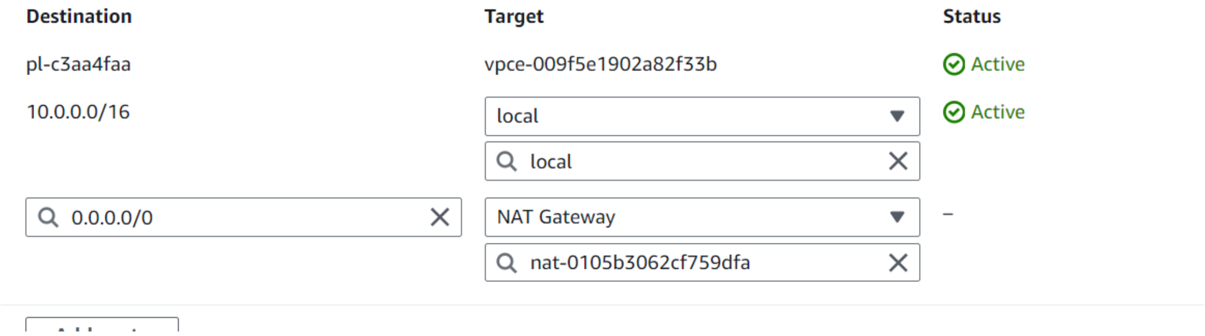
Stop to allow your instance to send and receive traffic when the source or destination is not itself.

☑ Stop

5. Go to **Route Tables** in **VPC**.
6. Select **Edit Routes.**



7. Select **0.0.0.0/0 – NAT GATEWAY**



Destination	Target	Status
pl-c3aa4faa	vpce-009f5e1902a82f33b	✓ Active
10.0.0.0/16	local ▼ local	✓ Active
0.0.0.0/0	NAT Gateway ▼ nat-0105b3062cf759dfa	–

8. CLICK ON **EDIT**
9. Have successfully launched **NAT INSTANCE.**