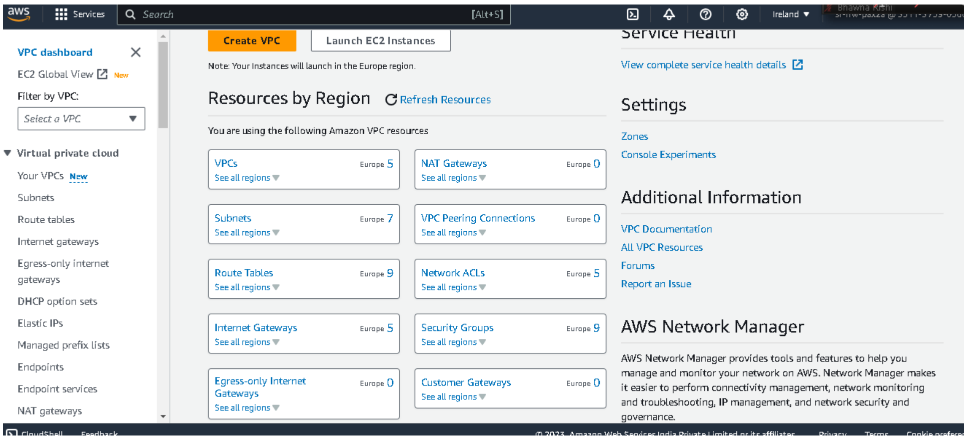
1. VPC ((Open aws then go to vpc-EC2))



Create VPC | Launch EC2 Instances

Note: Your Instances will launch in the Europe region.

Resources by Region — Refresh Resources

You are using the following Amazon VPC resources

VPCs See all regions	Europe 5	NAT Gateways See all regions	Europe 0
Subnets See all regions	Europe 7	VPC Peering Connections See all regions	Europe 0
Route Tables See all regions	Europe 9	Network ACLs See all regions	Europe 5
Internet Gateways See all regions	Europe 5	Security Groups See all regions	Europe 9
Egress-only Internet Gateways See all regions	Europe 0	Customer Gateways See all regions	Europe 0

Service Health

View complete service health details

Settings

Zones

Console Experiments

Additional Information

VPC Documentation

All VPC Resources

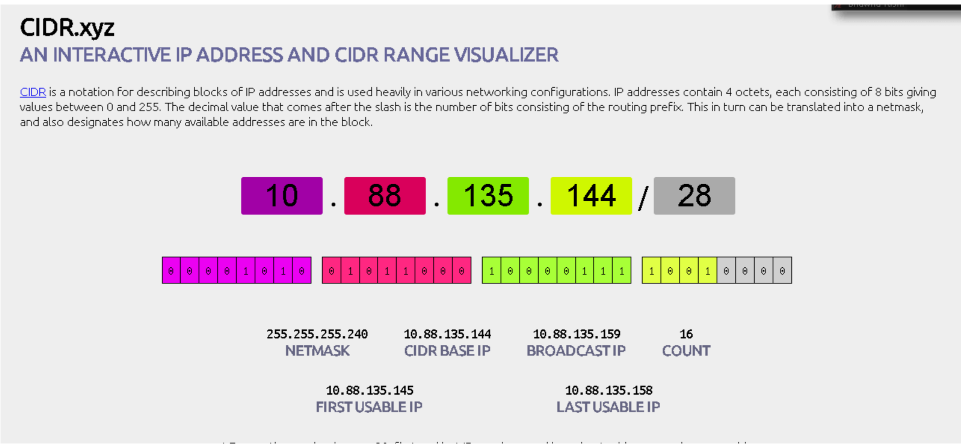
Forums

Report an Issue

AWS Network Manager

AWS Network Manager provides tools and features to help you manage and monitor your network on AWS. Network Manager makes it easier to perform connectivity management, network monitoring and troubleshooting, IP management, and network security and governance.

2. (Understanding of ip address)
https://cidr.xyz/



CIDR.xyz

AN INTERACTIVE IP ADDRESS AND CIDR RANGE VISUALIZER

CIDR is a notation for describing blocks of IP addresses and is used heavily in various networking configurations. IP addresses contain 4 octets, each consisting of 8 bits giving values between 0 and 255. The decimal value that comes after the slash is the number of bits consisting of the routing prefix. This in turn can be translated into a netmask, and also designates how many available addresses are in the block.

10 . 88 . 135 . 144 / 28

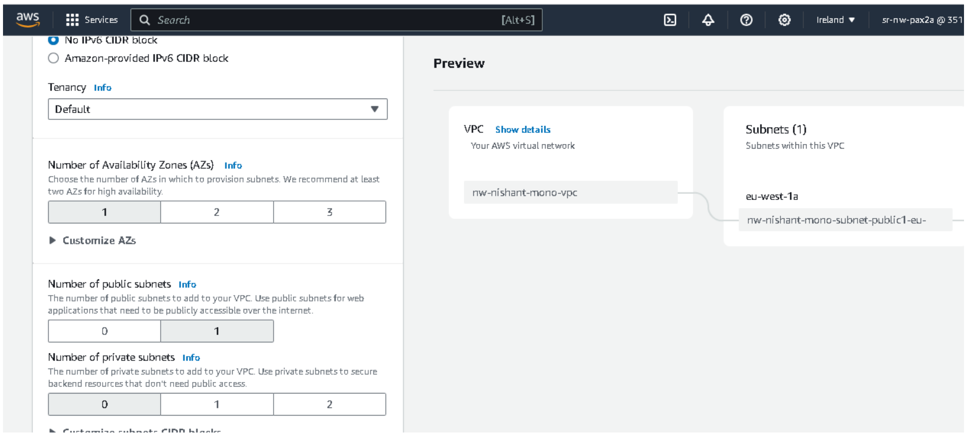
```
0 0 0 0 1 0 1 0   0 1 0 1 1 0 0 0   1 0 0 0 0 1 1 1   1 0 0 1 0 0 0 0
```

255.255.255.240 NETMASK	10.88.135.144 CIDR BASE IP	10.88.135.159 BROADCAST IP	16 COUNT

10.88.135.145 FIRST USABLE IP	10.88.135.158 LAST USABLE IP

3.

(Create VPC with below instructions)



● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

Tenancy Info
Default

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 [✓ 1]

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] 1 2

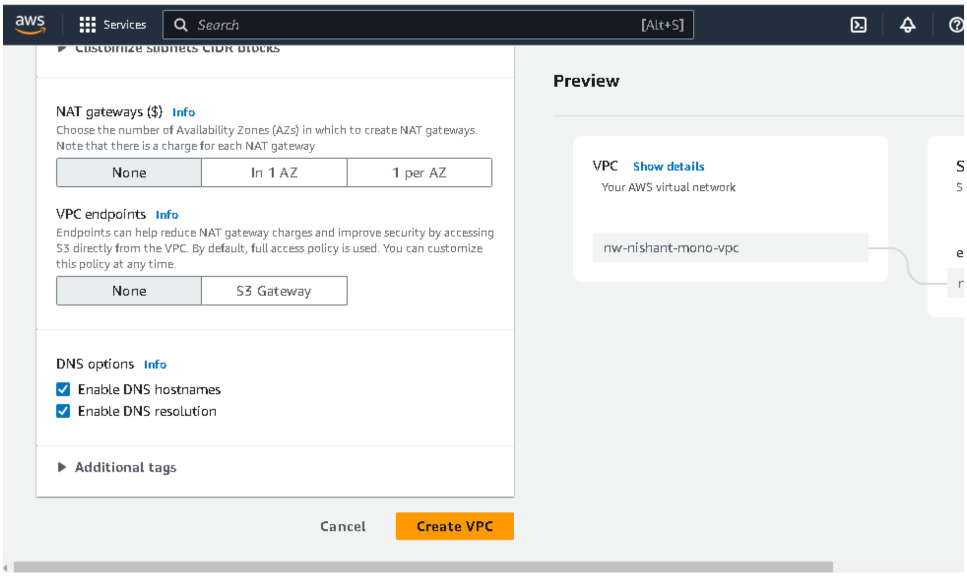
Customize subnets CIDR blocks

Preview

VPC Show details
Your AWS virtual network
nw-nishant-mono-vpc

Subnets (1)
Subnets within this VPC
eu-west-1a
nw-nishant-mono-subnet-public1-eu-

4.



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

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

[✓ None] S3 Gateway

DNS options Info

☑ Enable DNS hostnames

☑ Enable DNS resolution

Preview

VPC Show details

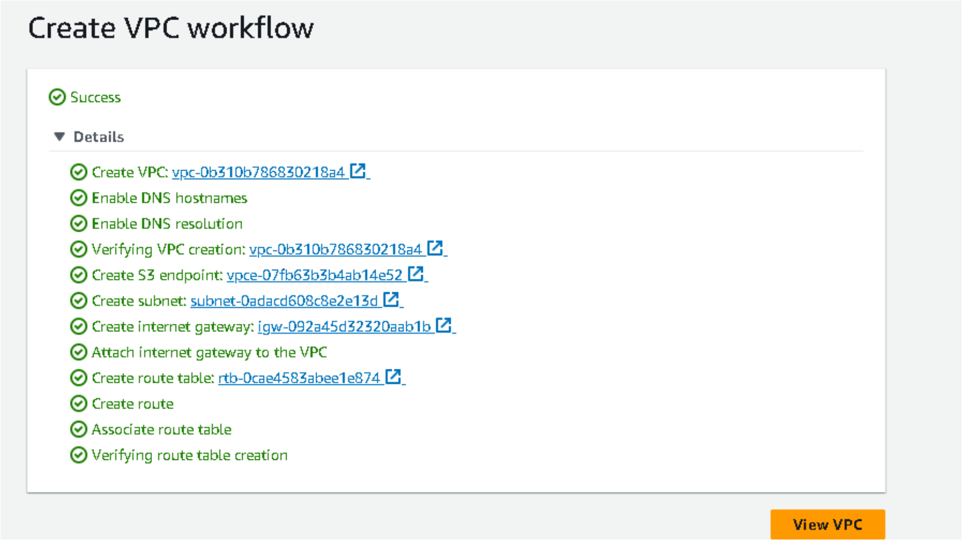
Your AWS virtual network

nw-nishant-mono-vpc

5.

[vpc-0b310b786830218a4]()

vpc-0b310b786830218a4

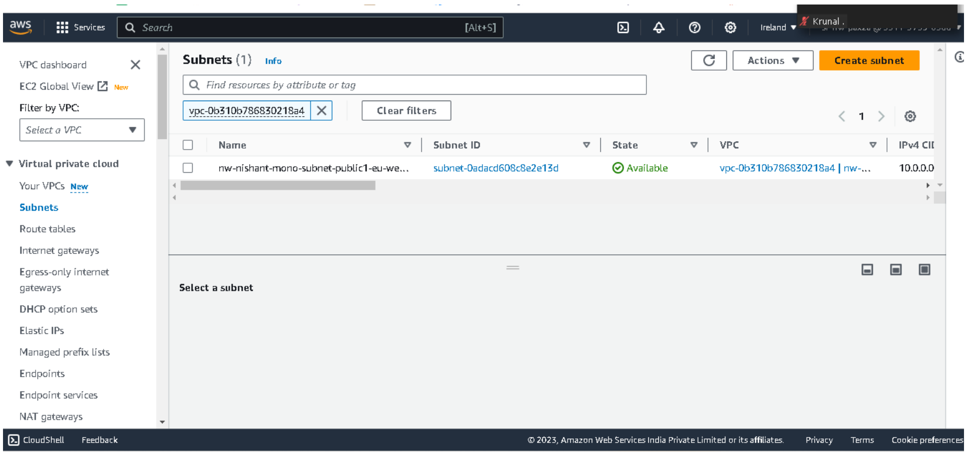


Create VPC workflow

✓ Success

Details

- ✓ Create VPC: vpc-0b310b786830218a4
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-0b310b786830218a4
- ✓ Create S3 endpoint: vpce-07fb63b3b4ab14e52
- ✓ Create subnet: subnet-0adacd608c8e2e13d
- ✓ Create internet gateway: igw-092a45d32320aab1b
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-0cae4583abee1e874
- ✓ Create route
- ✓ Associate route table
- ✓ Verifying route table creation



Subnets (1) Info

Find resources by attribute or tag

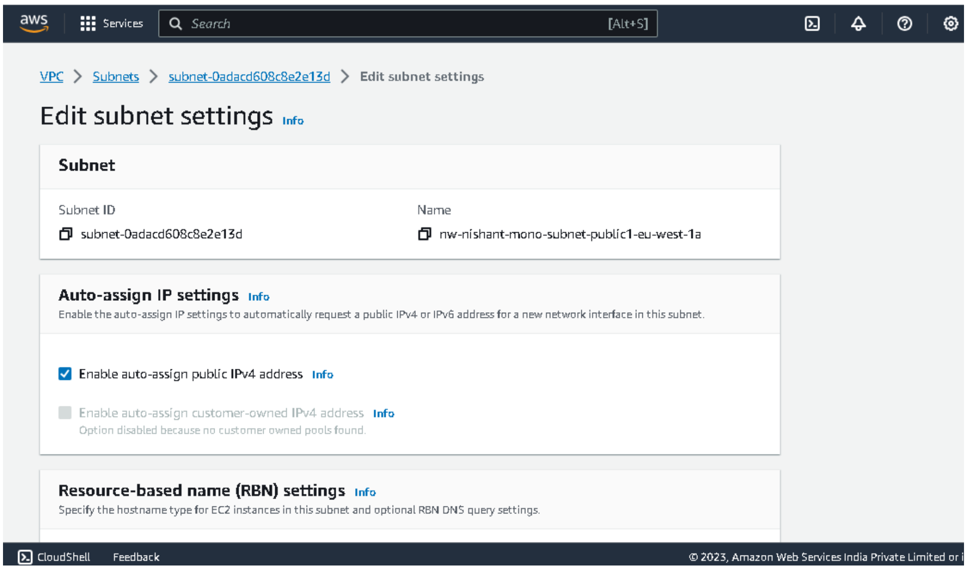
vpc-0b310b786830218a4

	Name	Subnet ID	State	VPC	IPv4 CI
□	nw-nishant-mono-subnet-public1-eu-we...	subnet-0adacd608c8e2e13d	✓ Available	vpc-0b310b786830218a4 | nw-...	10.0.0.0

Select a subnet

© 2023, Amazon Web Services India Private Limited or its affiliates.

6.


VPC > Subnets > subnet-0adacd608c8e2e13d > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID: subnet-0adacd608c8e2e13d

Name: nw-nishant-mono-subnet-public1-eu-west-1a

Auto-assign IP settings Info

Enable the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

☑ Enable auto-assign public IPv4 address Info

□ Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

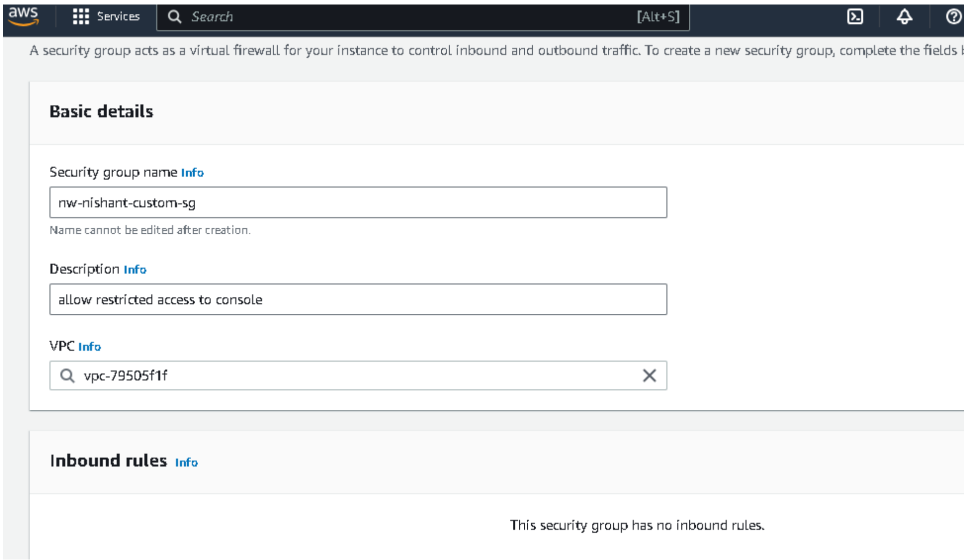
Resource-based name (RBN) settings Info

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

© 2023, Amazon Web Services India Private Limited or i

sg-0df33418868725632

7.


A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields b

Basic details

Security group name Info: nw-nishant-custom-sg
Name cannot be edited after creation.

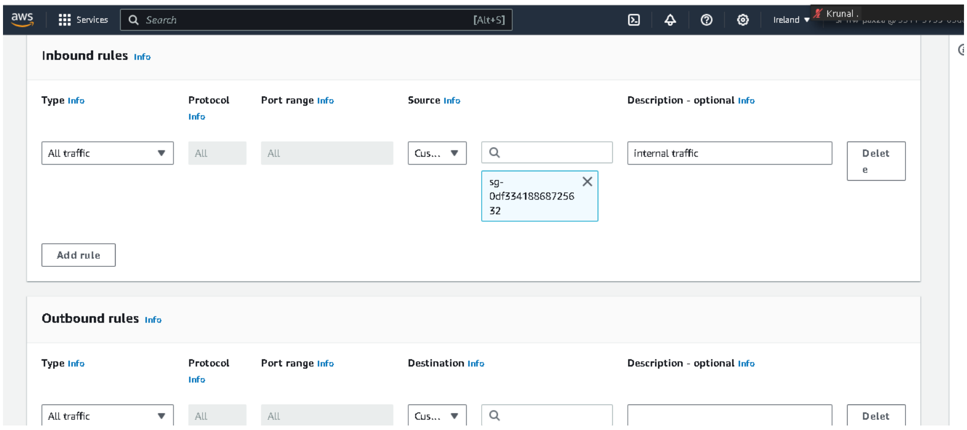
Description Info: allow restricted access to console

VPC Info: vpc-79505f1f

Inbound rules Info

This security group has no inbound rules.

8.


Inbound rules Info

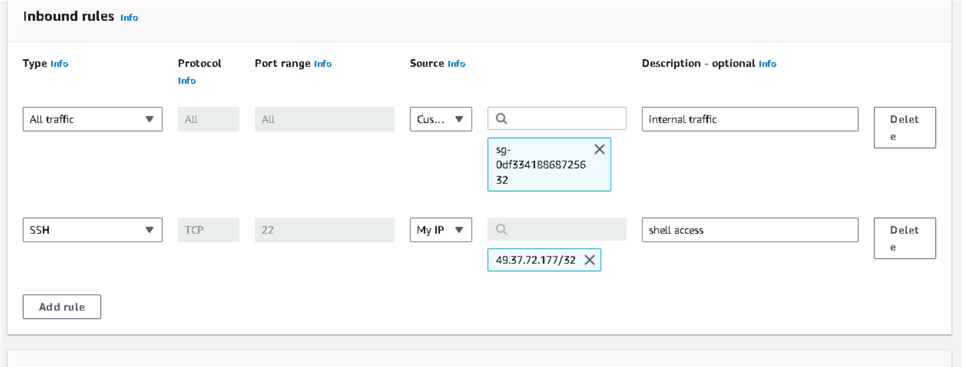
Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
All traffic	All	All	Cus...	sg-0df334188687256 32	internal traffic	Delete

Add rule

Outbound rules Info

Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info	
All traffic	All	All	Cus...			Delet

9.

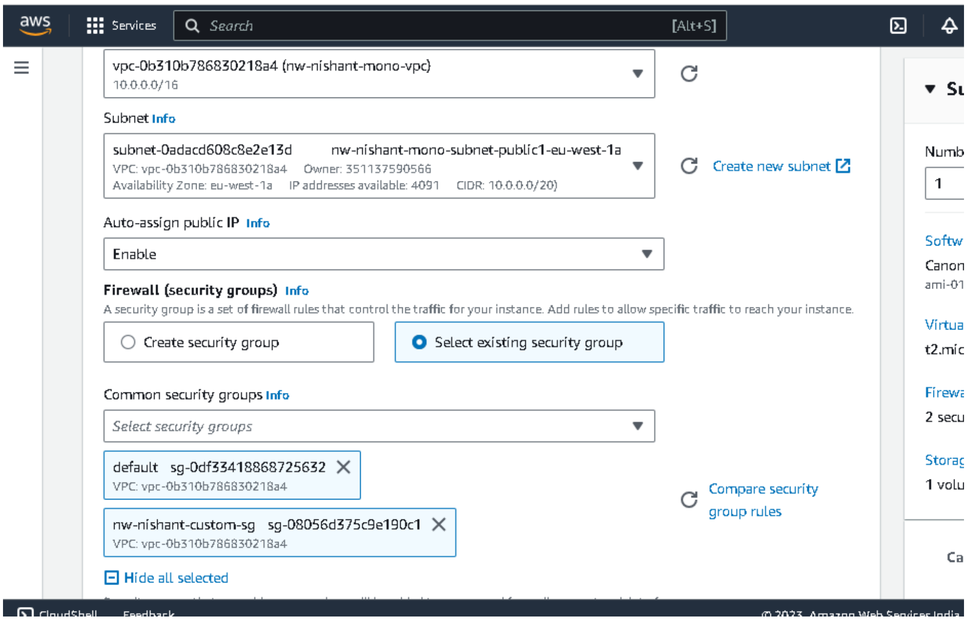


Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
All traffic	All	All	Cus...	sg-0df33418868725632	internal traffic	Delete
SSH	TCP	22	My IP	49.37.72.177/32	shell access	Delete

Add rule

10: create new instance in EC2.



vpc-0b310b786830218a4 (nw-nishant-mono-vpc)
10.0.0.0/16

Subnet Info

subnet-0adacd608c8e2e13d nw-nishant-mono-subnet-public1-eu-west-1a
VPC: vpc-0b310b786830218a4 Owner: 351137590566
Availability Zone: eu-west-1a IP addresses available: 4091 CIDR: 10.0.0.0/20)

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

Common security groups Info

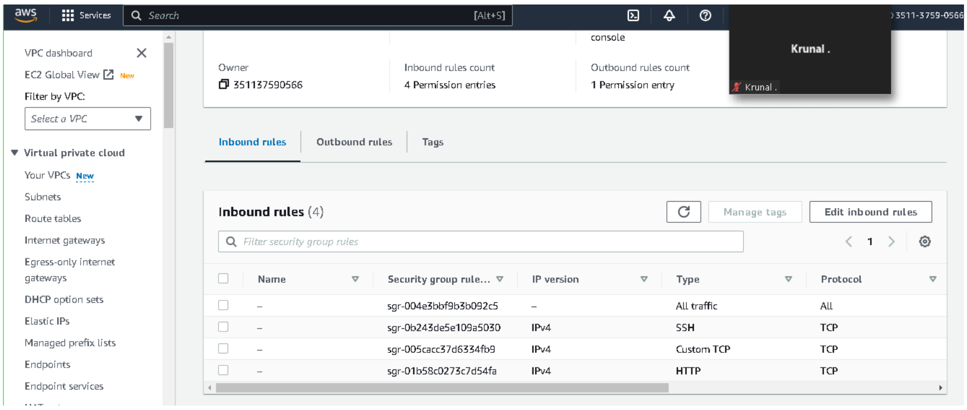
Select security groups

default sg-0df33418868725632
VPC: vpc-0b310b786830218a4

nw-nishant-custom-sg sg-08056d375c9e190c1
VPC: vpc-0b310b786830218a4

Compare security group rules

Hide all selected



Owner	Inbound rules count	Outbound rules count
351137590566	4 Permission entries	1 Permission entry

Inbound rules (4)

Name	Security group rule...	IP version	Type	Protocol
–	sgr-004e3bbf9b3b092c5	–	All traffic	All
–	sgr-0b243de5e109a5030	IPv4	SSH	TCP
–	sgr-005cacc37d6334fb9	IPv4	Custom TCP	TCP
–	sgr-01b58c0273c7d54fa	IPv4	HTTP	TCP

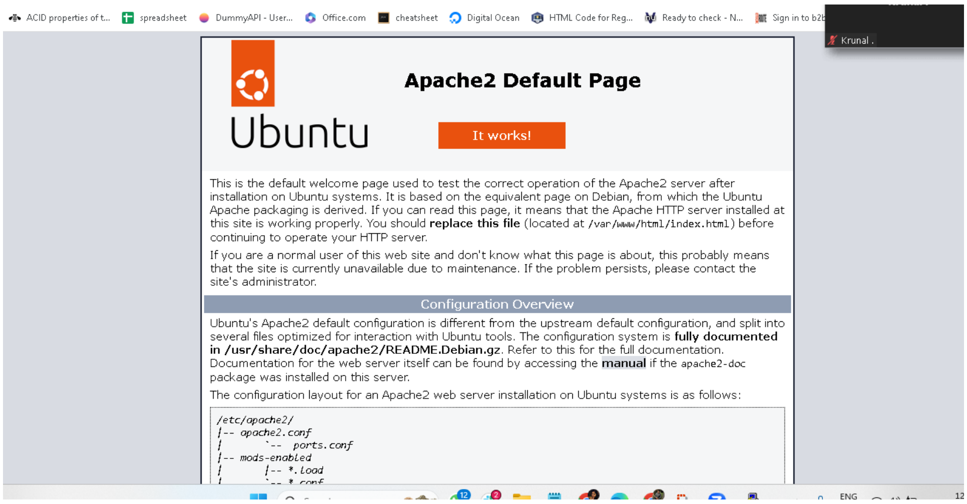
11: i-0a9593834a95d309e

Open putty

: sudo apt update

: sudo apt install apache2 –y

12:



Apache2 Default Page

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

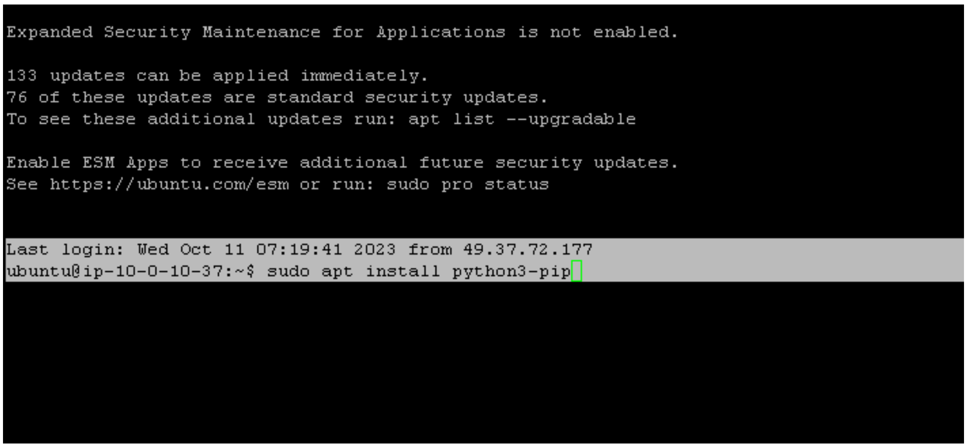
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
```

13.

Setup jupyterlab

Install python

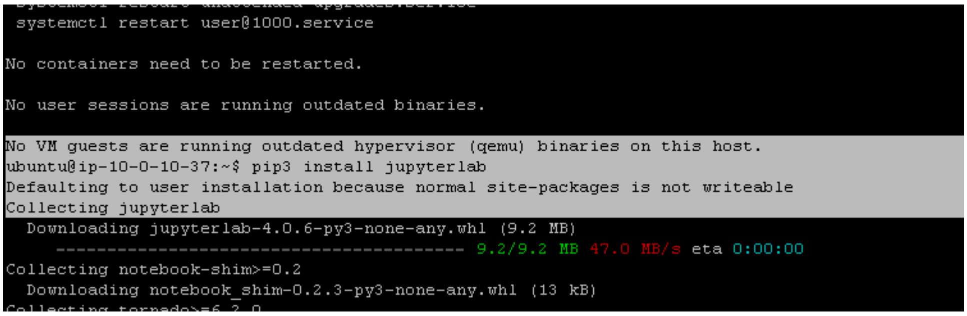


```
Expanded Security Maintenance for Applications is not enabled.

133 updates can be applied immediately.
76 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Wed Oct 11 07:19:41 2023 from 49.37.72.177
ubuntu@ip-10-0-10-37:~$ sudo apt install python3-pip
```

14.

Pip3 install jupyterlab

Sudo apt update



```
 systemctl restart user@1000.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-10-0-10-37:~$ pip3 install jupyterlab
Defaulting to user installation because normal site-packages is not writeable
Collecting jupyterlab
  Downloading jupyterlab-4.0.6-py3-none-any.whl (9.2 MB)
     ---------------------------------------- 9.2/9.2 MB 47.0 MB/s eta 0:00:00
Collecting notebook-shim>=0.2
  Downloading notebook_shim-0.2.3-py3-none-any.whl (13 kB)
Collecting tornado>=6.2.0
```

15.

Exec bash

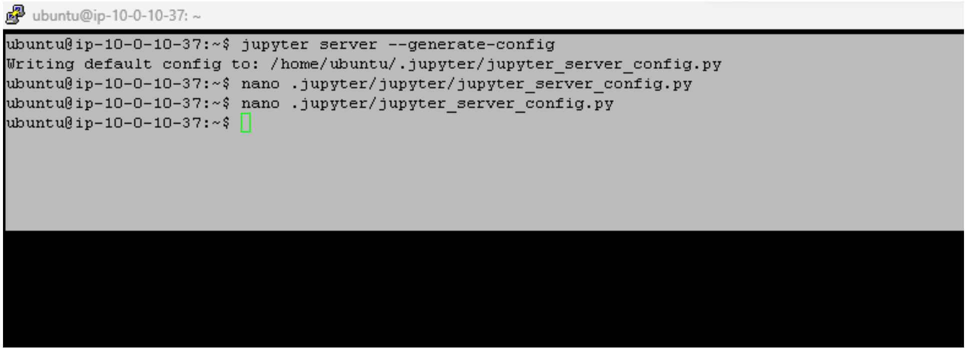
Exit

Reopen putty

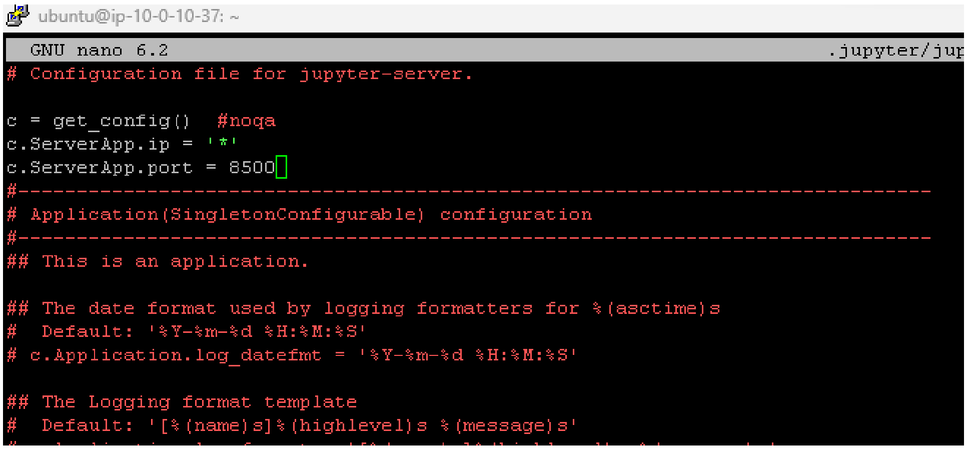
16.

Jupyter server –generate-config

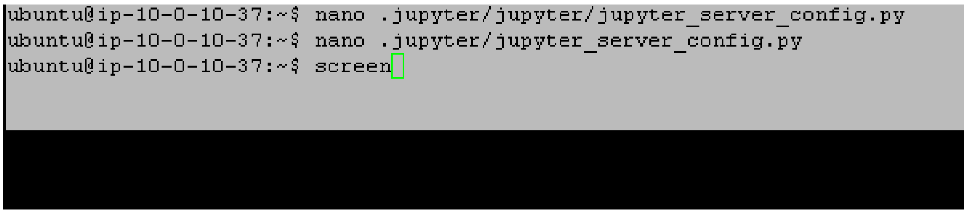
Nano .jupyter/jupyter_server_config.py



```
ubuntu@ip-10-0-10-37:~$ jupyter server --generate-config
Writing default config to: /home/ubuntu/.jupyter/jupyter_server_config.py
ubuntu@ip-10-0-10-37:~$ nano .jupyter/jupyter/jupyter_server_config.py
ubuntu@ip-10-0-10-37:~$ nano .jupyter/jupyter_server_config.py
ubuntu@ip-10-0-10-37:~$ 
```



```
  GNU nano 6.2                                                          .jupyter/jup
# Configuration file for jupyter-server.

c = get_config()  #noqa
c.ServerApp.ip = '*'
c.ServerApp.port = 8500
#------------------------------------------------------------------------------
# Application(SingletonConfigurable) configuration
#------------------------------------------------------------------------------
## This is an application.

## The date format used by logging formatters for %(asctime)s
#  Default: '%Y-%m-%d %H:%M:%S'
# c.Application.log_datefmt = '%Y-%m-%d %H:%M:%S'

## The Logging format template
#  Default: '[%(name)s]%(highlevel)s %(message)s'
```

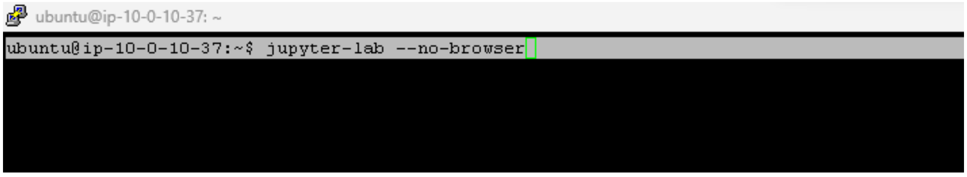


```
ubuntu@ip-10-0-10-37:~$ nano .jupyter/jupyter/jupyter_server_config.py
ubuntu@ip-10-0-10-37:~$ nano .jupyter/jupyter_server_config.py
ubuntu@ip-10-0-10-37:~$ screen
```

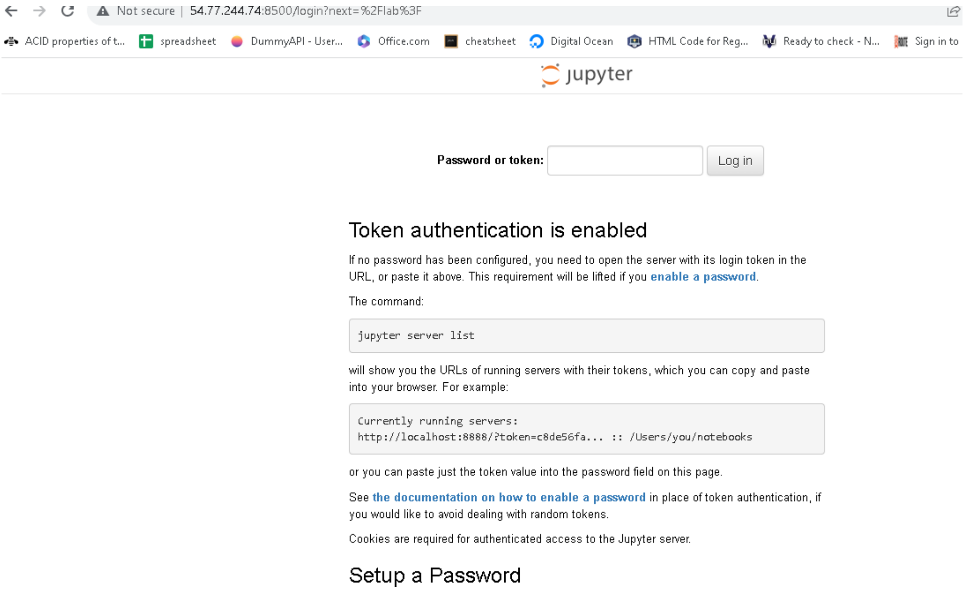
Screen

2 times space

Jupyter-lab --no-browser



```
ubuntu@ip-10-0-10-37:~$ jupyter-lab --no-browser
```


Not secure | 54.77.244.74:8500/login?next=%2Flab%3F
ACID properties of t... spreadsheet DummyAPI - User... Office.com cheatsheet Digital Ocean HTML Code for Reg... Ready to check - N... Sign in to
jupyter
Log in

Password or token:

Token authentication is enabled

If no password has been configured, you need to open the server with its login token in the URL, or paste it above. This requirement will be lifted if you **enable a password**.

The command:

```
jupyter server list
```

will show you the URLs of running servers with their tokens, which you can copy and paste into your browser. For example:

```
Currently running servers:
http://localhost:8888/?token=c8de56fa... :: /Users/you/notebooks
```

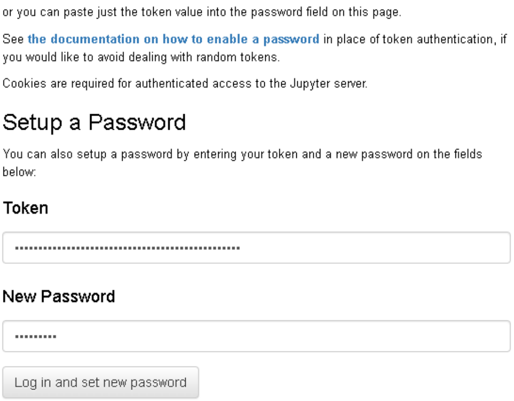
or you can paste just the token value into the password field on this page.

See **the documentation on how to enable a password** in place of token authentication, if you would like to avoid dealing with random tokens.

Cookies are required for authenticated access to the Jupyter server.

Setup a Password

Token no: b674d25cbf5965e42f73f7f786b93fd2482185e6d5066fdc



or you can paste just the token value into the password field on this page.

See **the documentation on how to enable a password** in place of token authentication, if you would like to avoid dealing with random tokens.

Cookies are required for authenticated access to the Jupyter server.

Setup a Password

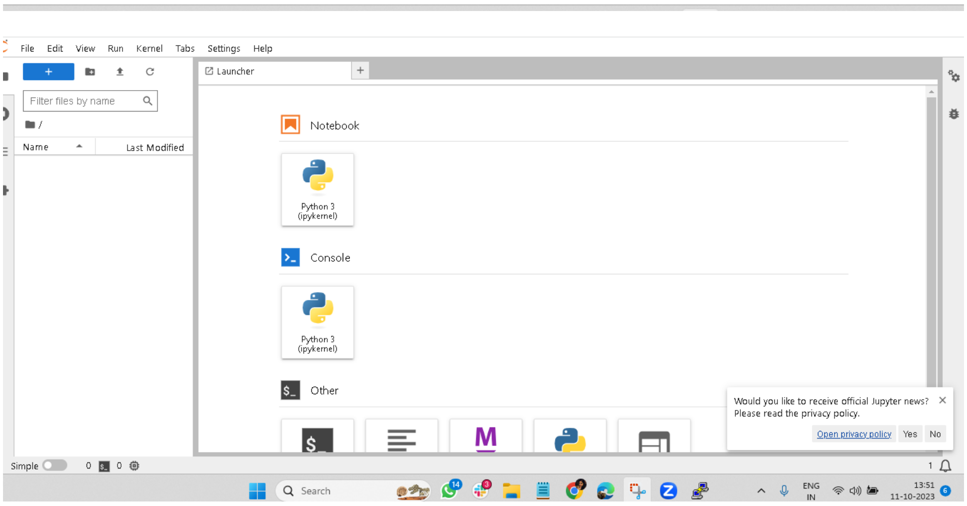
You can also setup a password by entering your token and a new password on the fields below:

Token

••

New Password

•••••••••



Would you like to receive official Jupyter news?
Please read the privacy policy.