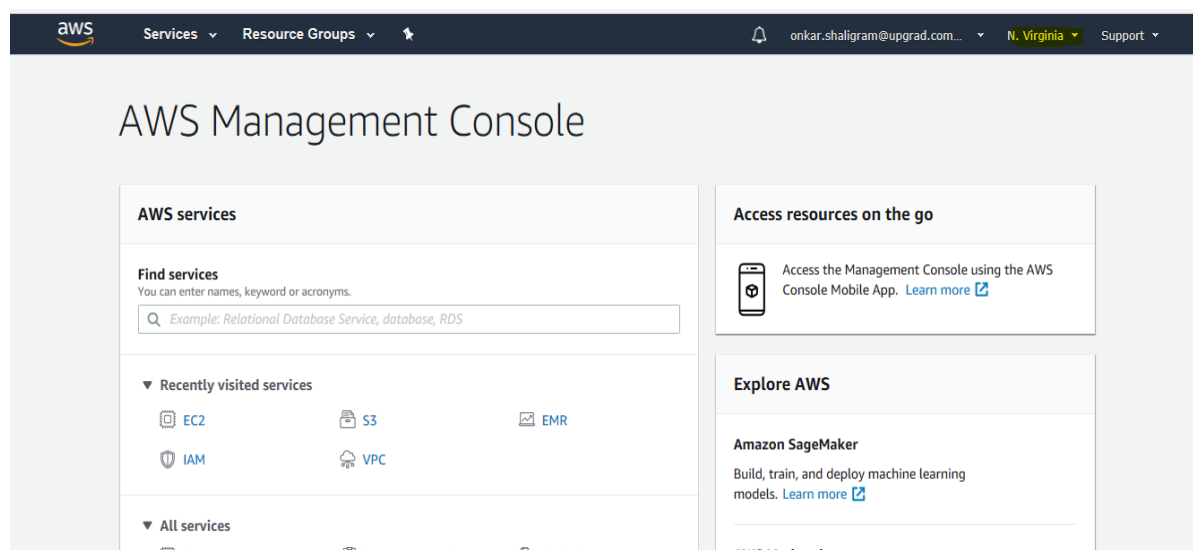


Steps for Creating VPC and Security Group

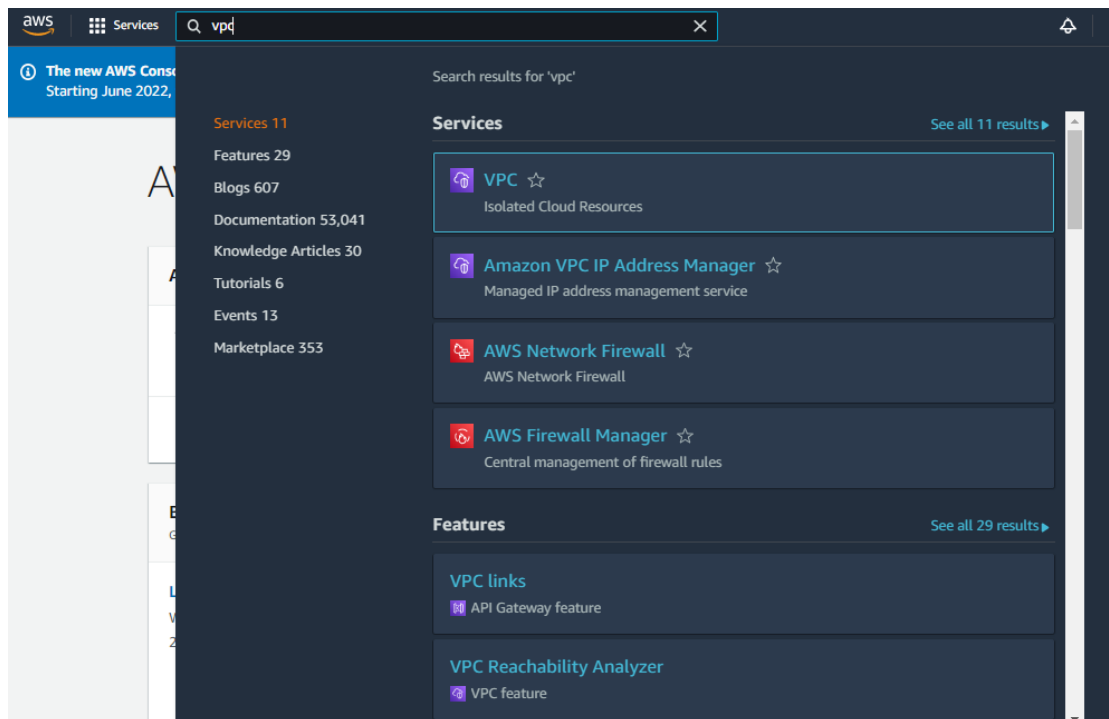
The Amazon VPC allows users to provision an isolated section of AWS according to their requirement. Users can utilize the resources of AWS in a virtual network. They can also customize their virtual environment according to their needs.

Note: The VPC setup is a one time process and you can make use of the VPC created here in the instances that you'll launch in the future.

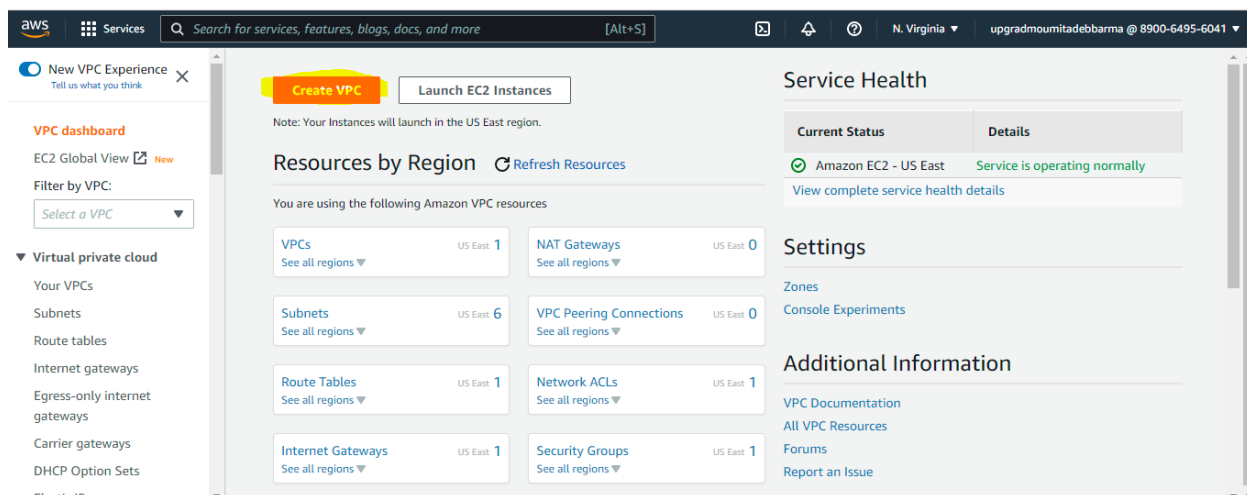
1. Enter your AWS Console using NuvePro dashboard.
2. You will see AWS Console Home, which will look like the following image:
(Set the Region to **N.Virginia**)



3. In the **search** tab section, type “**VPC**”. Click on enter.



4. Now the VPC dashboard opens. Click on “**Create VPC**”



5. The following page below will now open up. Navigate to the right side of the page to update the settings for the vpc.

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

Introducing the new create VPC experience

We've designed the new create VPC to make it easier to use. The changes include a new visualization of the resources that will be created. Let us know what you think.

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

IPv4 CIDR block [Info](#)

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

65,536 IPs

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Preview

VPC [show details](#)

Your AWS virtual network

my-vpc-vpc

Subnets (1)

Subnets within this VPC

us-east-1a

my-vpc-subnet-public1-us-east-1a

Route tables (1)

Route network traffic to resources

my-vpc-rtb-public

Network connections (1)

Connections to other networks

my-vpc-igw

6. Click on “VPC and more” and assign the below values:

Check Auto-generate: **my-vpc**

IPv4 CIDR: **10.0.0.0/16**

Number of Availability Zones(AZs): **1**

Number of public subnet: **1**

Number of private subnet: **0**

Nat Gateway: **None**

Vpc endpoint: **none**

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

IPv4 CIDR block [Info](#)

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

65,536 IPs

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

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

► 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
------	---------	----------

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


Cancel

Create VPC

7. Click on the “Create VPC” button and now your VPC will be created.

VPC > Your VPCs > Create VPC > Create VPC resources

Create VPC workflow


Creating VPC Resources
×

Thank you for using the new create VPC experience. Let us know what you think.

✓ Success

▼ Details

- ✓ Create VPC: [vpc-0cf77ae1b1863c7a2](#)
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: [vpc-0cf77ae1b1863c7a2](#)
- ✓ Create subnet: [subnet-0f4e6fc27eaf09bdd](#)
- ✓ Create internet gateway: [igw-09050da1e810d38c2](#)
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: [rtb-01c8825c00e94d77d](#)
- ✓ Create route
- ✓ Associate route table
- ✓ Verifying route table creation

[View VPC](#)

8. The VPC has been created successfully. Click on 'View VPC' to view the VPC.

NOTE: Please note that an extra “vpc” will be appended at the end of the vpc name you’ve created. Additionally, please note down the unique VPC ids of your newly created VPCs.

VPC > Your VPCs > [vpc-0cf77ae1b1863c7a2](#)

vpc-0cf77ae1b1863c7a2 / my-vpc-vpc

Actions ▼

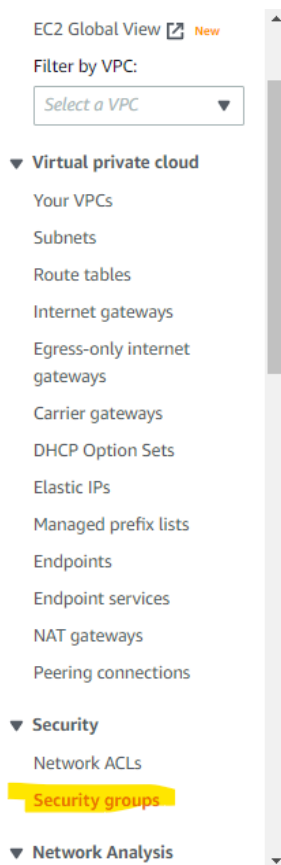
Details [Info](#)

VPC ID  vpc-0cf77ae1b1863c7a2	State ✓ Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-158fbb6e	Main route table rtb-09549f97b4a41d0fb	Main network ACL acl-08c6f9a52c1b3ee34
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Route 53 Resolver DNS Firewall rule groups -	Owner ID  986167097117		

Now we need to create a new security group inside our VPC.

Creating a Security Group.

1. Inside the VPC dashboard, Go to the left side page and click on the **security group**.



2. Click on “create security group”

Security Groups (3) Info						
<input type="text" value="Filter security groups"/>		Actions		Export security groups to CSV		Create security group
<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input type="checkbox"/>	-	sg-0ec77d570c4c842d6	default	vpc-09f16d6f0ced234f4	default VPC security gr...	986167097117
<input type="checkbox"/>	-	sg-0e4571062d36d265d	default	vpc-0049757136cf4a0de	default VPC security gr...	986167097117
<input type="checkbox"/>	-	sg-47fa7001	default	vpc-37ba304d	default VPC security gr...	986167097117

3. Give the **security group name**, **description** and our **vpc name**(my-vpc-vpc).
- NOTE:** Recheck the VPC id to make sure that you’re choosing the correct VPC.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

vpc-0cf77ae1b1863c7a2 (my-vpc-vpc)
10.0.0.0/16
vpc-37ba304d (default)
172.31.0.0/16

4. Click on “create security group” and then click on “close”.

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info	
All traffic ▼	All	All	Custom ▼ <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<input type="button" value="Delete"/>
<input type="button" value="Add rule"/>					

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add up to 50 more tags

Security group (sg-0a5d749a76e37e6e5 | my-vpc-security) was created successfully

Details

VPC > Security Groups > sg-0a5d749a76e37e6e5 - my-vpc-security

sg-0a5d749a76e37e6e5 - my-vpc-security

Actions

Details			
Security group name my-vpc-security	Security group ID sg-0a5d749a76e37e6e5	Description Security group for my vpc	VPC ID vpc-0cf77ae1b1863c7a2
Owner 986167097117	Inbound rules count 0 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

Inbound rules [Manage tags](#) [Edit inbound rules](#)

Filter security group rules

- Select the Security group you've created and scroll down then **click on inbound rules** and then **edit rules**.

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

Inbound rules [Manage tags](#) [Edit inbound rules](#)

Filter security group rules

	Name	Security group rule...	IP version	Type	Protocol	Port range
No security group rules found						

- Click on **"Add Rules"**

VPC > Security Groups > sg-0a5d749a76e37e6e5 - my-vpc-security > Edit inbound rules

Edit inbound rules info

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

Inbound rules info

This security group has no inbound rules.

[Add rule](#)

Cancel [Preview changes](#) [Save rules](#)

7. **Select Type** to be “**ALL TCP**” The **source** should be “**My IP address only**”, finally click on “**save rules.**”

VPC > Security Groups > sg-0a5d749a76e37e6e5 - my-vpc-security > 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>	
-	All TCP	TCP	0 - 65535	My IP		Delete

[Add rule](#)

Cancel [Preview changes](#) [Save rules](#)

Note: Inside the Source, My IP should be the same as IP shown on the given website.
<https://www.ip2location.com/>

8. The security group with the updated details would be visible now.

sg-0a5d749a76e37e6e5 - my-vpc-security [Actions](#)

Details

Security group name my-vpc-security	Security group ID sg-0a5d749a76e37e6e5	Description Security group for my vpc	VPC ID vpc-0cf77ae1b1863c7a2
Owner 986167097117	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

[Inbound rules](#) [Outbound rules](#) [Tags](#)

ⓘ You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#) [×](#)

Inbound rules (1/1) [Manage tags](#) [Edit inbound rules](#)

<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range
<input checked="" type="checkbox"/>	-	sgr-0b3aba869bd520e...	IPv4	All TCP	TCP	0 - 65535

NOTE: Refrain from putting myip address for the outboundrules. Add rules> Anywhere IPv4

Edit outbound rules
[info](#)

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules
[info](#)

Security group rule ID	Type info	Protocol info	Port range info	Destination info	Description - optional info
sgr-01d2558ae179250da	All traffic	All	All	Anywh...	

10. Now back to the services and **search “EC2”** to create the instance.

