

We will now create a security group inside our VPC.

## Creating a Security Group.

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

The screenshot shows the AWS VPC console. On the left sidebar, under the 'SECURITY' section, 'Security Groups' is highlighted in yellow. The main content area shows 'Your VPCs (4)' with a table listing VPCs. The 'upgrad\_vpc' is selected.

Name	VPC ID	State
upgrad_vpc	vpc-04ae0ba72672f7c0a	Available
-	vpc-63d8021e	Available

2. Click on “**create security group**”

The screenshot shows the AWS Security Groups console. The 'Create security group' button is highlighted in yellow. The table below lists existing security groups.

Name	Security group ID	Security group name	VPC ID	Description
-	sg-00d8899ea1410c650	launch-wizard-2	vpc-63d8021e	launch-wizard-2 create.
-	sg-0126270472319ab38	default	vpc-0746afceb9aaaa6ee	default VPC security gr.
-	sg-01564417467886e6a	launch-wizard-4	vpc-63d8021e	launch-wizard-4 create.
-	sg-0256dde26b4403025	launch-wizard-3	vpc-63d8021e	launch-wizard-3 create.

3. Give the **security group name, description** and our **vpc name**(upgrad\_vpc).

VPC > Security Groups > Create security group

## Create security group [Info](#)

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 following steps:

### Basic details

Security group name [Info](#)

mongo-db-security-group

Name cannot be edited after creation.

Description [Info](#)

security group

VPC [Info](#)

vpc-04ae0ba72672f7c0a (upgrad\_vpc)

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

aws Services Resource Groups

onkar.shaligram@upgrad.com... N. Virginia Support

Security Groups > Create security group

### Create security group

✓ The following security group was created:

Security Group ID sg-0dd5c69ad227a0d25

Close

5. Select the Security group “**mongo-db-security-group**” and scroll down then **click on inbound rules** and then **edit rules**.

Security Groups (1/27) [Info](#)

Filter security groups

	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input type="checkbox"/>	-	sg-00a960a38e8723935	Kafka_demo	vpc-0d5c826a35153dfef	launch-wizard-9 create...	9112685088
<input type="checkbox"/>	-	sg-00d8899ea1410c650	launch-wizard-2	vpc-63d8021e	launch-wizard-2 create...	9112685088
<input type="checkbox"/>	-	sg-0126270472319ab38	default	vpc-0746afceb9aaaa6ee	default VPC security gr...	9112685088
<input type="checkbox"/>	-	sg-01564417467886e6a	launch-wizard-4	vpc-63d8021e	launch-wizard-4 create...	9112685088
<input type="checkbox"/>	-	sg-0256dde26b4403025	launch-wizard-3	vpc-63d8021e	launch-wizard-3 create...	9112685088
<input type="checkbox"/>	-	sg-037d5e580c0bdba05	ElasticMapReduce-mas...	vpc-63d8021e	Master group for Elasti...	9112685088
<input checked="" type="checkbox"/>	mongo-db-security...	sg-0464016716307dd4b	mongo-db-security-gr...	vpc-0d5c826a35153dfef	Security Group	9112685088

sg-0464016716307dd4b - mongo-db-security-group

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

sg-0464016716307dd4b - mongo-db-security-group

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

Inbound rules (1) [Edit inbound rules](#)

## 6. Click on “Add Rules”

aws Services Resource Groups

onkar.shaligram@upgrad.com... N. Virginia Support

Security Groups > Edit inbound rules

### Edit inbound rules

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

Type	Protocol	Port Range	Source	Description
This security group has no rules				

[Add Rule](#)

## 7. Select Type to be “ALL TCP”

Security Groups > Edit inbound rules

### Edit inbound rules

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

Type	Protocol	Port Range	Source	Description
All TCP	TCP	0 - 65535	Custom CIDR, IP, Security Group or Prefix List	e.g. SSH for Admin Desktop

Filter by attributes

- Custom Protocol
- All TCP
- All UDP
- All ICMP - IPv4
- All ICMP - IPv6
- All traffic
- SSH

rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period.

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

## 8. The **source** should be “My IP” address only, finally click on “save rules.”

Security Groups > Edit inbound rules

### Edit inbound rules

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

Type	Protocol	Port Range	Source	Description
All TCP	TCP	0 - 65535	My IP	125.99.155.86/32
				e.g. SSH for Admin Desktop

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

\* Required

Cancel Save rules

## 9. Click on “close”



Security Groups > Edit inbound rules

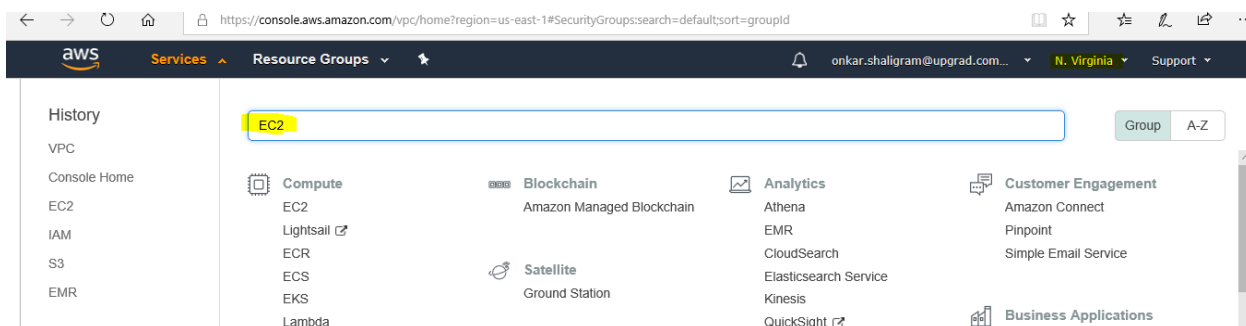
### Edit inbound rules

✓ Inbound security group rules successfully edited

Close

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

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



**Disclaimer:** All content and material on the upGrad website is copyrighted material, either belonging to upGrad or its bonafide contributors and is purely for the dissemination of education. You are permitted to access print and download extracts from this site purely for your own education only and on the following basis:

- You can download this document from the website for self-use only.
- Any copies of this document, in part or full, saved to disc or to any other storage medium may only be used for subsequent, self-viewing purposes or to print an individual extract or copy for non-commercial personal use only.
- Any further dissemination, distribution, reproduction, copying of the content of the document herein or the uploading thereof on other websites or use of the content for any other commercial/unauthorized purposes in any way which could infringe the intellectual property rights of upGrad or its contributors, is strictly prohibited.
- No graphics, images or photographs from any accompanying text in this document will be used separately for unauthorised purposes.
- No material in this document will be modified, adapted or altered in any way.
- No part of this document or upGrad content may be reproduced or stored in any other web site or included in any public or private electronic retrieval system or service without upGrad's prior written permission.
- Any rights not expressly granted in these terms are reserved.