

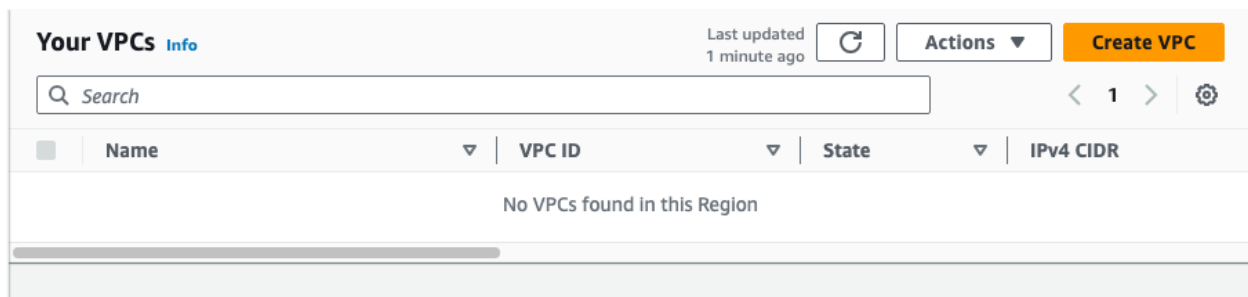
# Virtual Private Network & Security Groups

<b>VPC</b>	<b>1</b>
<b>Security Group for ALB</b>	<b>6</b>
<b>Security Group for Application / Backend Microservices</b>	<b>7</b>
<b>Security Group for DB</b>	<b>8</b>

---

## VPC

- Delete the default VPC to avoid confusion.
  - No worries, you can always create the default VPC when you need it!
- Let's start from scratch.



- VPC Settings
  - I give the VPC name as “netflux”.

### 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

netflux

**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

CIDR block size must be between /16 and /28.

**IPv6 CIDR block** [Info](#)

☒ No IPv6 CIDR block ☐ Amazon-provided IPv6 CIDR block

**Tenancy** [Info](#)

Default

- For high availability, let's use at least 2 AZs.

**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

**First availability zone**

us-east-1a

**Second availability zone**

us-east-1b

- We need
  - 2 public subnets. 1 for each AZ.
  - 2 private subnets for our backend microservices. 1 for each AZ.
  - 2 DB subnets.

### 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

Public subnet CIDR block in us-east-1a

10.0.1.0/24

256 IPs

Public subnet CIDR block in us-east-1b

10.0.2.0/24

256 IPs

Private subnet CIDR block in us-east-1a

10.0.3.0/24

256 IPs

Private subnet CIDR block in us-east-1b

10.0.4.0/24

256 IPs

Private subnet CIDR block in us-east-1a

10.0.5.0/24

256 IPs

Private subnet CIDR block in us-east-1b

10.0.6.0/24

256 IPs

- We also need a NAT gateway. **It costs money.** We can do it later when the time comes! Let's ignore it for now.
  - Enable the DNS options.

### 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.

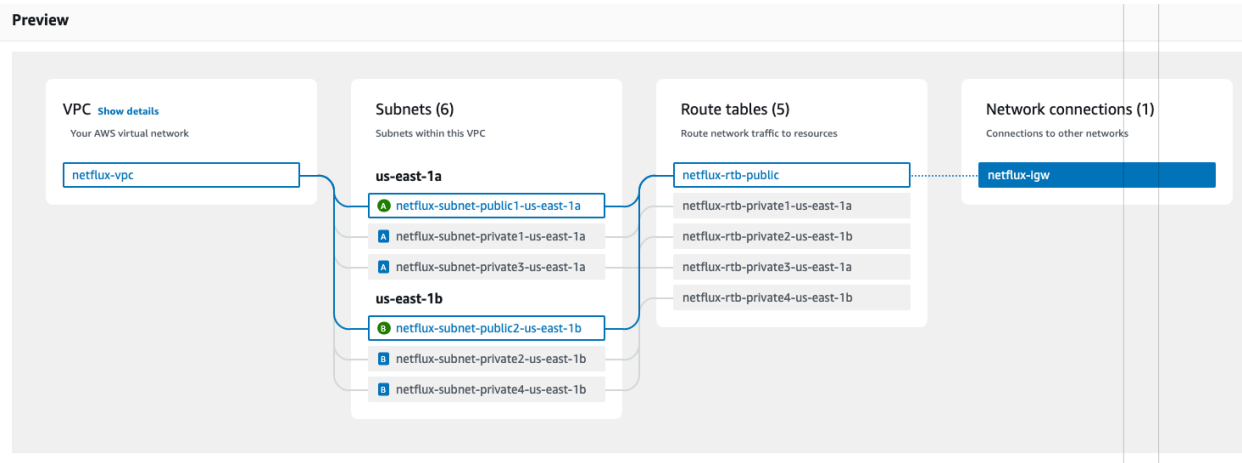
None

S3 Gateway

### DNS options [Info](#)

- ☒ Enable DNS hostnames
- ☒ Enable DNS resolution

- The network we create would look like this.



- Create VPC.
- Once it is created, do a “hard browser refresh”. AWS Console refresh does NOT seem to work well in some cases.

Verify What We Have Created:

- VPC

Your VPCs (1) <a href="#">Info</a>					Last updated 1 minute ago	<a href="#">Refresh</a>	<a href="#">Actions</a>	<a href="#">Create VPC</a>
<input type="text" value="Search"/>								
<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR				
<input type="checkbox"/>	netflux-vpc	<a href="#">vpc-057e4b12c96c3791e</a>	Available	10.0.0.0/16				

- Subnets

## Subnets (6) [Info](#)

Last updated  
3 minutes ago



Actions ▾

Create subnet

Find resources by attribute or tag

< 1 > ⚙

<input type="checkbox"/>	Name ▾	Subn... ▾	State ▾	VPC ▾	IPv4 CIDR
<input type="checkbox"/>	netflux-subnet-public1-us-east-1a	<a href="#">subnet-...</a>	✓ Available	<a href="#">vpc-057...</a>	10.0.1.0/24
<input type="checkbox"/>	netflux-subnet-public2-us-east-1b	<a href="#">subnet-...</a>	✓ Available	<a href="#">vpc-057...</a>	10.0.2.0/24
<input type="checkbox"/>	netflux-subnet-private1-us-east-1a	<a href="#">subnet-...</a>	✓ Available	<a href="#">vpc-057...</a>	10.0.3.0/24
<input type="checkbox"/>	netflux-subnet-private2-us-east-1b	<a href="#">subnet-...</a>	✓ Available	<a href="#">vpc-057...</a>	10.0.4.0/24
<input type="checkbox"/>	netflux-subnet-private3-us-east-1a	<a href="#">subnet-...</a>	✓ Available	<a href="#">vpc-057...</a>	10.0.5.0/24
<input type="checkbox"/>	netflux-subnet-private4-us-east-1b	<a href="#">subnet-...</a>	✓ Available	<a href="#">vpc-057...</a>	10.0.6.0/24

- Internet Gateway should have been attached to the VPC.

## Internet gateways (1) [Info](#)



Actions ▾

Create Internet gateway

Search

< 1 > ⚙

<input type="checkbox"/>	Name ▾	Internet gateway ID ▾	State ▾	VPC ID
<input type="checkbox"/>	netflux-igw	<a href="#">igw-0e547ddfec4ff09c9</a>	✓ Attached	<a href="#">vpc-057e4b12c96c3791e</a>

- Check the route tables. The public route table should have a route to 0.0.0.0/0 to Internet Gateway.

[VPC](#) > [Route tables](#) > [rtb-0f91cdbbc5c46136f](#)

## rtb-0f91cdbbc5c46136f / netflux-rtb-public

Actions ▾

### Details [Info](#)

Route table ID

rtb-0f91cdbbc5c46136f

Main

No

Explicit subnet associations

[2 subnets](#)

Edge associations

–

VPC

[vpc-057e4b12c96c3791e](#) |  
[netflux-vpc](#)

Owner ID

941077029185

[Routes](#)

[Subnet associations](#)

[Edge associations](#)

[Route propagation](#)

[Tags](#)

### Routes (2)

Both ▾

Edit routes

Filter routes

< 1 > ⚙

Destination ▾	Target ▾	Status
0.0.0.0/0	<a href="#">igw-0e547ddfec4ff09c9</a>	✓ Active
10.0.0.0/16	local	✓ Active

- Check the subnets association. 2 public subnets should have been associated with this route table!

Routes	<b>Subnet associations</b>	Edge associations	Route propagation	Tags
--------	----------------------------	-------------------	-------------------	------

<b>Explicit subnet associations (2)</b>				<a href="#">Edit subnet associations</a>
<input type="text" value="Find subnet association"/>				< 1 > ⚙
Name ▾	Subnet ID ▾	IPv4 CIDR ▾	IPv6 CIDR ▾	
netflux-subnet-public2-us-e...	<a href="#">subnet-07253a8d320578845</a>	10.0.2.0/24	–	
netflux-subnet-public1-us-e...	<a href="#">subnet-05b695fccfbce21ee</a>	10.0.1.0/24	–	

- **Network ACL.** By default we allow all the inbound requests!

Details

**Inbound rules**

Outbound rules

Subnet associations

Tags

**Inbound rules (2)**

Edit inbound rules

🔍

Filter inbound rules

< 1 >

⚙

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✔ Allow
*	All traffic	All	All	0.0.0.0/0	✘ Deny

## Security Groups

- We need 3 security groups.
  - external traffic → ALB → APP → DB

### Security Group for ALB

Security group name [Info](#)  
  
Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)  
 ▾

- Inbound Rule
  - allow requests from anywhere 0.0.0.0/0 for port 80

**Inbound rules** [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
HTTP ▼	TCP	80	Anyw... ▼	0.0.0.0/0	0.0.0.0/0 ✕
<div>Add rule</div> <div>Delete</div>					

## Security Group for Application / Backend Microservices

**Security group name** [Info](#)

netflux-app-sg

Name cannot be edited after creation.

**Description** [Info](#)

allow traffic from alb to app

**VPC** [Info](#)

vpc-057e4b12c96c3791e (netflux-vpc) ▼

- Inbound Rule to allow traffic from ALB.
  - Port: **8080**
  - Source: Select the “**netflux-alb-sg**”

**Inbound rules** [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
Custom TCP ▼	TCP	8080	Custom ▼	netflux-alb-sg   sg-0a799e4078dcfad76	default   sg-01ced0f2b0aec83db
<div>Add rule</div> <div>Delete</div>					

- Create the Security Group
- Remember that apps can talk among themselves! **customer-service** will want to talk to **movie-service** to get the movie information. However the current rule is explicitly to allow the traffic only from ALB. So, let's add another inbound rule.
- Click on “Edit Inbound Rules” to add another rule as shown below.

We allow 8080 among backend applications

**Inbound rules** [Info](#)

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>
sgr-0ad8abbaf924eac9a	Custom TCP ▼	TCP	8080	Custom ▼
sgr-0944b18a24fa888c4	Custom TCP ▼	TCP	8080	Custom ▼

Add rule

**Security Groups**

default | sg-052d9357f58dea35b

netflux-alb-sg | sg-01c508c6bb7c98235

netflux-app-sg | sg-0a323d530be8b5c8e

netflux-app-sg | sg-0a323d530be8b5c8e

**Prefix lists**

com.amazonaws.us-east-1.dynamodb | pl-0...

com.amazonaws.us-east-1.ipv6.route53-hea

## Security Group for DB

- Enter the details

**Security group name** [Info](#)

netflux-db-sg

Name cannot be edited after creation.

**Description** [Info](#)

allow traffic from backend apps

**VPC** [Info](#)

vpc-057e4b12c96c3791e (netflux-vpc) ▼

- We add this inbound rule.
  - port: **5432**
  - source: “**netflux-app-sg**”

**Inbound rules** [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>
Custom TCP ▼	TCP	5432	Custom ▼

Add rule

**Security Groups**

netflux-app-sg | sg-0f8140a3ae11308ee

default | sg-01ced0f2b0aec83db

netflux-alb-sg | sg-0a799e4078dcfad76

**Prefix lists**

Delete