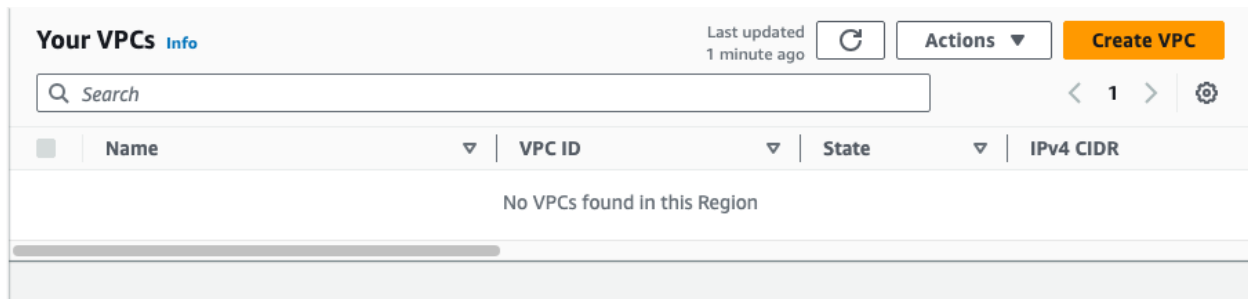


# Virtual Private Cloud

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



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

A screenshot of the AWS 'VPC settings' configuration page. The title is 'VPC settings'. Under 'Resources to create', there are two radio buttons: 'VPC only' and 'VPC and more' (which is selected). The 'Name tag auto-generation' section has a checked 'Auto-generate' checkbox and a text input field containing 'netflux'. The 'IPv4 CIDR block' section has a text input field containing '10.0.0.0/16' and a note that the CIDR block size must be between /16 and /28. The 'IPv6 CIDR block' section has two radio buttons: 'No IPv6 CIDR block' (selected) and 'Amazon-provided IPv6 CIDR block'. The 'Tenancy' section has a dropdown menu set to '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

use1-az1 (us-east-1a) ▼

##### Second availability zone

use1-az2 (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. We also do NOT need **S3 Gateway**,

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.

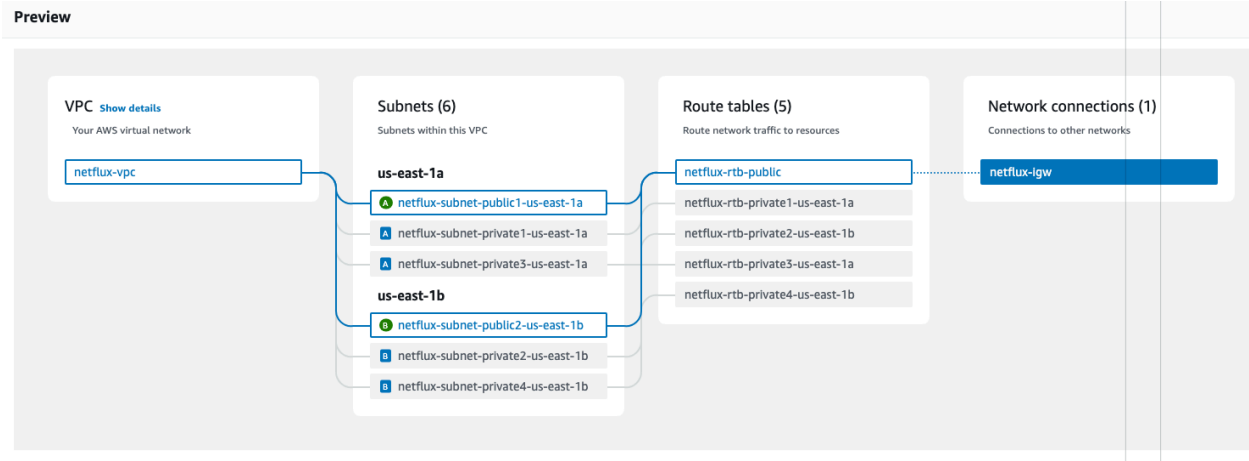
**None** | S3 Gateway

- Ensure that these DNS options are selected.

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) [Info](#)

Last updated 1 minute ago [Refresh](#) [Actions](#) [Create VPC](#)

<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 [Refresh](#) [Actions](#) [Create subnet](#)

<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) <a href="#">Info</a>				
<input type="text" value="Search"/> <span>&lt; 1 &gt;</span>				
<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 <a href="#">2 subnets</a>	Edge associations -
VPC <a href="#">vpc-057e4b12c96c3791e</a> netflux-vpc	Owner ID 941077029185		

[Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

**Routes (2)** Both Edit 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!

<a href="#">Routes</a>   <a href="#">Subnet associations</a>   <a href="#">Edge associations</a>   <a href="#">Route propagation</a>   <a href="#">Tags</a>				
Explicit subnet associations (2) <span>Edit subnet associations</span>				
<input type="text" value="Find subnet association"/> <span>&lt; 1 &gt;</span>				
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-05b695fccfbc21ee</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