

# 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!

The screenshot shows the 'Your VPCs' page in the AWS VPC console. At the top, there is a search bar and a 'Create VPC' button. Below the search bar, there are columns for 'Name', 'VPC ID', 'State', and 'IPv4 CIDR'. A message 'No VPCs found in this Region' is displayed. The interface is clean and modern, typical of AWS management tools.

- VPC Settings
  - I give the VPC name as "netflix".

The screenshot shows the 'VPC settings' dialog. Under 'Resources to create', the 'VPC and more' option is selected. In the 'Name tag auto-generation' section, 'Auto-generate' is checked and the value 'netflix' is entered. Under 'IPv4 CIDR block', the value '10.0.0.0/16' is specified, which is noted to provide 65,536 IPs. The 'IPv6 CIDR block' section shows 'No IPv6 CIDR block' is selected. Finally, under 'Tenancy', 'Default' is chosen.

- 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.

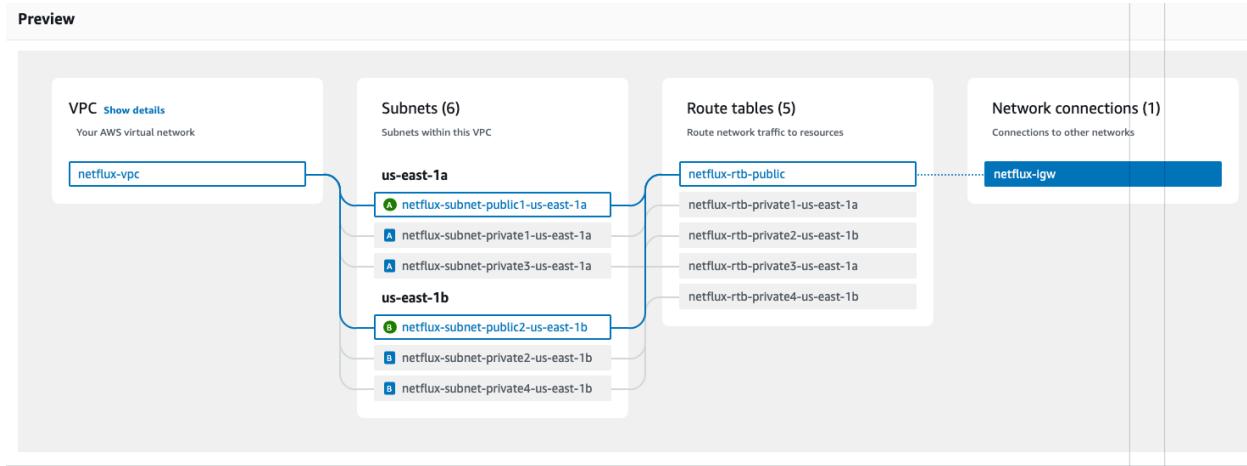
[None](#) | [S3 Gateway](#)

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

- Subnets

Subnets (6) <a href="#">Info</a>						Last updated 3 minutes ago	<a href="#">Actions</a>	<a href="#">Create subnet</a>
<input type="checkbox"/> <a href="#">Name</a> <a href="#">Subn...</a> <a href="#">State</a> <a href="#">VPC</a> <a href="#">IPv4 CIDR</a>							<a href="#">Actions</a>	<a href="#">Create subnet</a>
<input type="checkbox"/> <a href="#">Name</a> <a href="#">Subn...</a> <a href="#">State</a> <a href="#">VPC</a> <a href="#">IPv4 CIDR</a>							<a href="#">Actions</a>	<a href="#">Create subnet</a>
<input type="checkbox"/>	<a href="#">netflux-subnet-public1-us-east-1a</a>	<a href="#">subnet-...</a>	<span>Available</span>	<a href="#">vpc-057...</a>	<a href="#">10.0.1.0/24</a>			
<input type="checkbox"/>	<a href="#">netflux-subnet-public2-us-east-1b</a>	<a href="#">subnet-...</a>	<span>Available</span>	<a href="#">vpc-057...</a>	<a href="#">10.0.2.0/24</a>			
<input type="checkbox"/>	<a href="#">netflux-subnet-private1-us-east-1a</a>	<a href="#">subnet-...</a>	<span>Available</span>	<a href="#">vpc-057...</a>	<a href="#">10.0.3.0/24</a>			
<input type="checkbox"/>	<a href="#">netflux-subnet-private2-us-east-1b</a>	<a href="#">subnet-...</a>	<span>Available</span>	<a href="#">vpc-057...</a>	<a href="#">10.0.4.0/24</a>			
<input type="checkbox"/>	<a href="#">netflux-subnet-private3-us-east-1a</a>	<a href="#">subnet-...</a>	<span>Available</span>	<a href="#">vpc-057...</a>	<a href="#">10.0.5.0/24</a>			
<input type="checkbox"/>	<a href="#">netflux-subnet-private4-us-east-1b</a>	<a href="#">subnet-...</a>	<span>Available</span>	<a href="#">vpc-057...</a>	<a href="#">10.0.6.0/24</a>			

- Internet Gateway should have been attached to the VPC.

Internet gateways (1) <a href="#">Info</a>			
<input type="checkbox"/>	Name	Internet gateway ID	State
<input type="checkbox"/>	netflux-igw	<a href="#">igw-0e547ddfec4ff09c9</a>	Attached

- 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 / netflux-rtb-public [Actions](#)

Details <a href="#">Info</a>			
Route table ID	Main	Explicit subnet associations	Edge associations
<input type="checkbox"/> <a href="#">rtb-0f91cdbbc5c46136f</a>	<input type="checkbox"/> No	<a href="#">2 subnets</a>	-
VPC	Owner ID		
<a href="#">vpc-057e4b12c96c3791e   netflux-vpc</a>	<input type="checkbox"/> 941077029185		

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

Routes (2)		
<a href="#">Edit routes</a>		
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 style="float: right;"><a href="#">Edit subnet associations</a></span>					
<a href="#">Find subnet association</a> <span style="float: right;"><a href="#">Edit subnet associations</a></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-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
<b>Inbound rules (2)</b>				
<input type="text"/> Filter inbound rules				
Rule number	Type	Protocol	Port range	Source
100	All traffic	All	All	0.0.0.0/0
*	All traffic	All	All	0.0.0.0/0
				Allow/Deny
				<input checked="" type="checkbox"/> Allow
				<input type="checkbox"/> Deny