NextWork.org

Build a Virtual Private Cloud

Anitta Philip


Anitta Philip
https://www.linkedin.com/in/anittap/

Introducing Amazon VPC!

What it does & how it’s useful

Amazon Virtual Private Cloud (VPC) is a customizable network space in AWS that allows you to launch AWS resources in a virtual network. Developers and teams use Amazon VPC because it offers isolation, security, and control over network configurations.

How I’m using it in today’s project

I’m using Amazon VPC in this project to demonstrate how to create a customizable network space in AWS, set up subnets, and attach an internet gateway. This tutorial aims to provide a step-by-step guide for enabling auto-assign public IPs and configuring network settings.

This project took me...

The project took me less than an hour to complete. Documentation took me less than an hour to write as well.


Anitta Philip
https://www.linkedin.com/in/anittap/

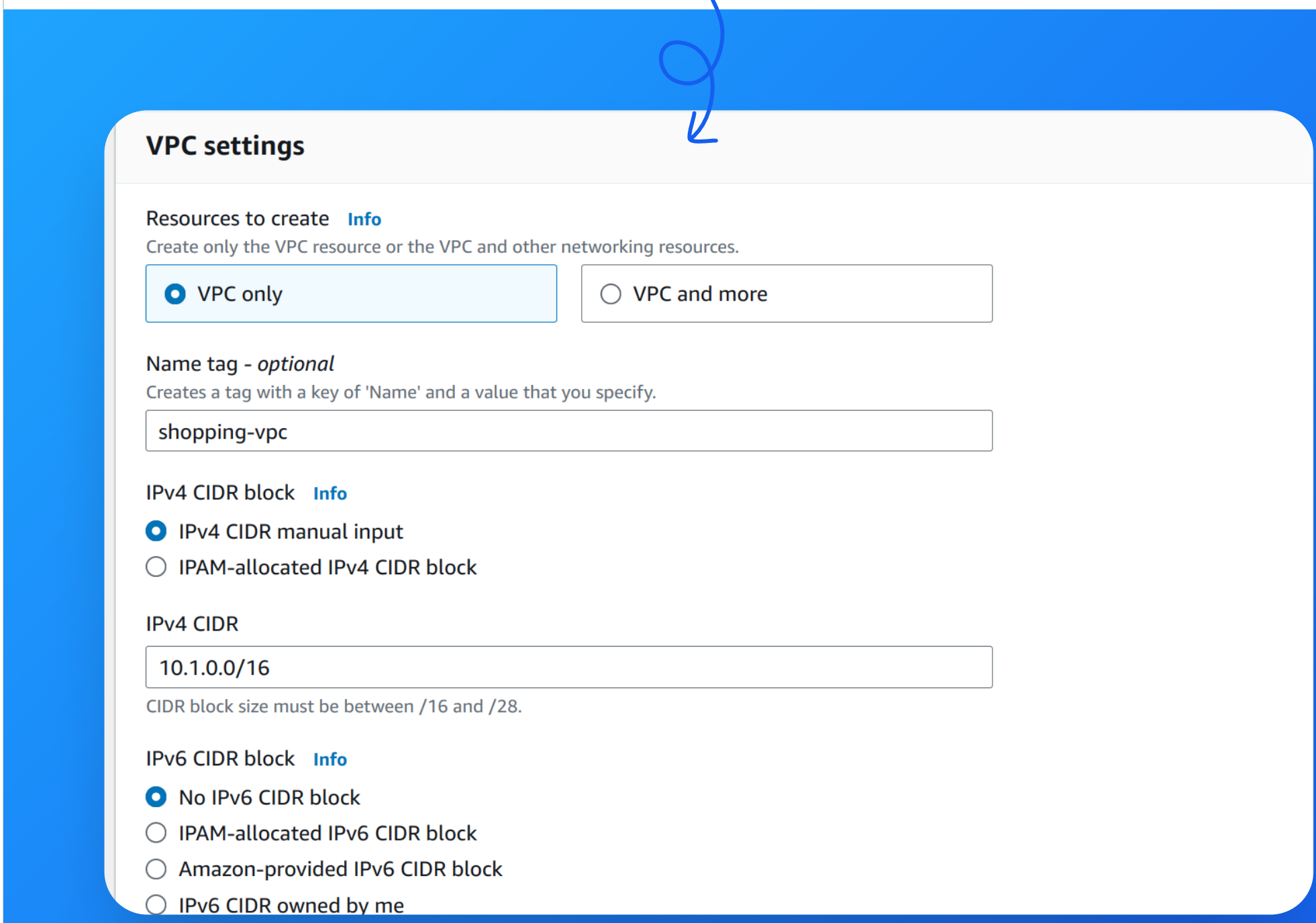
My first VPC

VPCs are customizable network spaces in AWS that allow you to launch and manage AWS resources within a virtual network.

There was already a default VPC in my account ever since my AWS account was created. This is because AWS automatically provides a default VPC in each region to simplify networking setup for new users.

To set up my VPC, I had to define an IPv4 CIDR, which means specifying an IP address range for the network, such as 10.1.0.0/16, to segment and organize the network space efficiently.

My VPC setup page




Anitta Philip
https://www.linkedin.com/in/anittap/

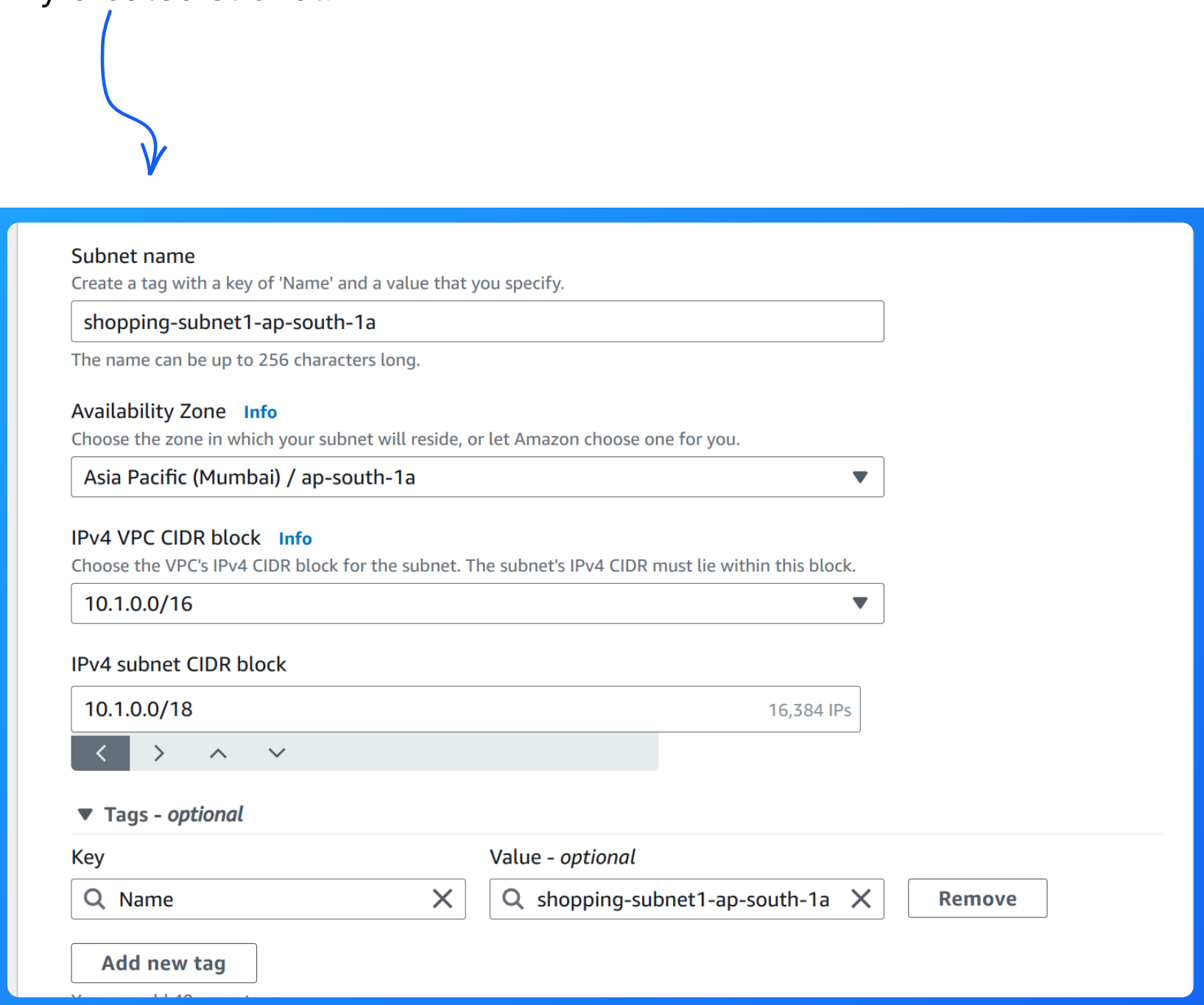
Subnets

- Subnets are subdivisions of a VPC's IP address range, used to segment the network for better management and security.

- There are already subnets existing in my account, one for every availability zone in the region. AWS provides multiple subnets to enhance redundancy and availability of resources.

- For a subnet to be considered public, it has to be associated with a route table that has a route to an internet gateway. Conversely, subnets without such a route are private subnets.

My created subnet!



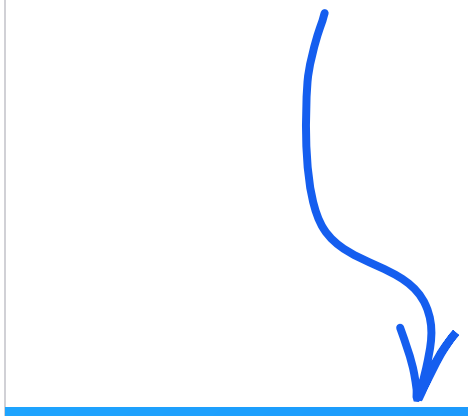
Anitta Philip
https://www.linkedin.com/in/anittap/

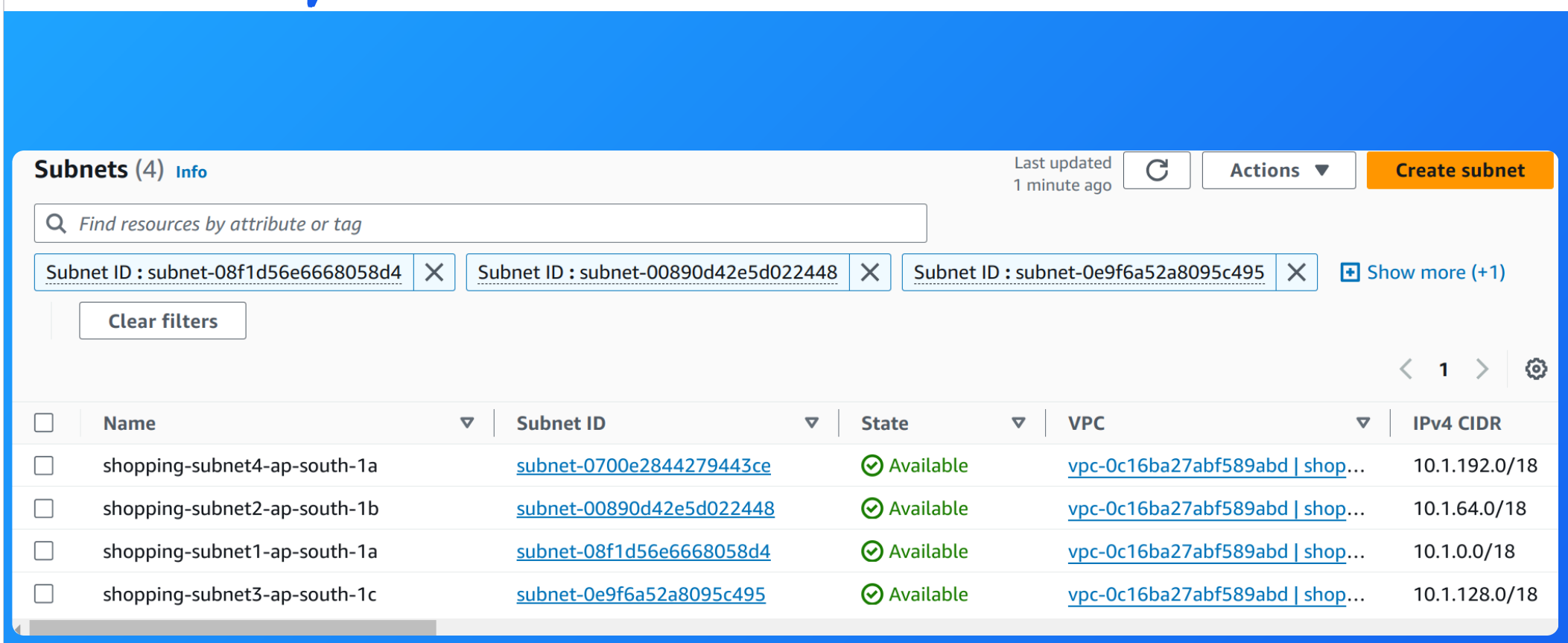
I created four subnets in total: two in ap-south-1a, one in ap-south-1b, and one in ap-south-1c, leveraging all three availability zones in the Mumbai region. The subnets are as follows:

- ap-south-1a: 10.1.0.0/18 and 10.1.192.0/18
- ap-south-1b: 10.1.64.0/18
- ap-south-1c: 10.1.128.0/18

I chose these IP ranges to ensure even distribution and to maximize the available IP addresses within the VPC. Using a Class A IP range (10.1.0.0/16) offers the benefit of a larger address space, which is advantageous for scalability and flexibility in a growing network.

Multiple subnets can be attached to the same availability zone, as I did with ap-south-1a. However, this can lead to potential resource contention and less fault tolerance within that zone. It's important to balance subnets across availability zones to avoid single points of failure.





Anitta Philip
https://www.linkedin.com/in/anittap/

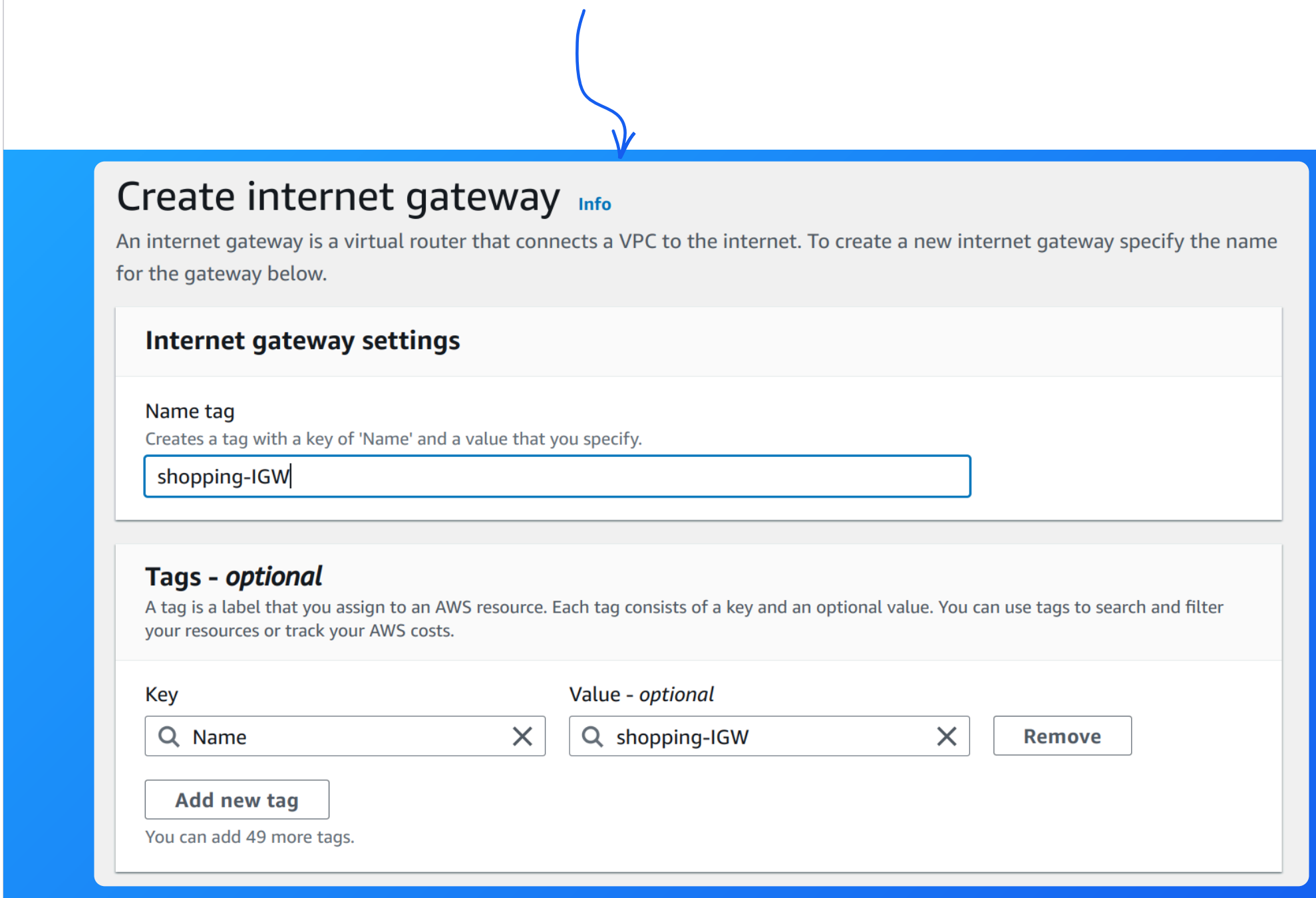
Internet gateways

- Internet gateways are AWS-managed resources that allow instances within a VPC to connect to the Internet.

- Attaching an internet gateway to a VPC means enabling internet connectivity for instances within the VPC that have public IP addresses assigned.

- While I've set up an internet gateway and attached it to a VPC, I still have to set up route tables. Route tables will need to be configured to direct internet-bound traffic (`0.0.0.0/0`) to the attached internet gateway, enabling instances to communicate with the internet

My created internet gateway!



Anitta Philip
https://www.linkedin.com/in/anittap/

Attach to vpc

Now we need to attach the newly created internet gateway to our vpc.

To attach an internet gateway to a vpc :

- Right-click on the Internet gateway
- Select attach to VPC
- Select the VPC > Attach internet gateway

By following these steps, you enable internet connectivity for your VPC instances, allowing them to access the internet and be accessed from the internet if they have public IP addresses assigned.

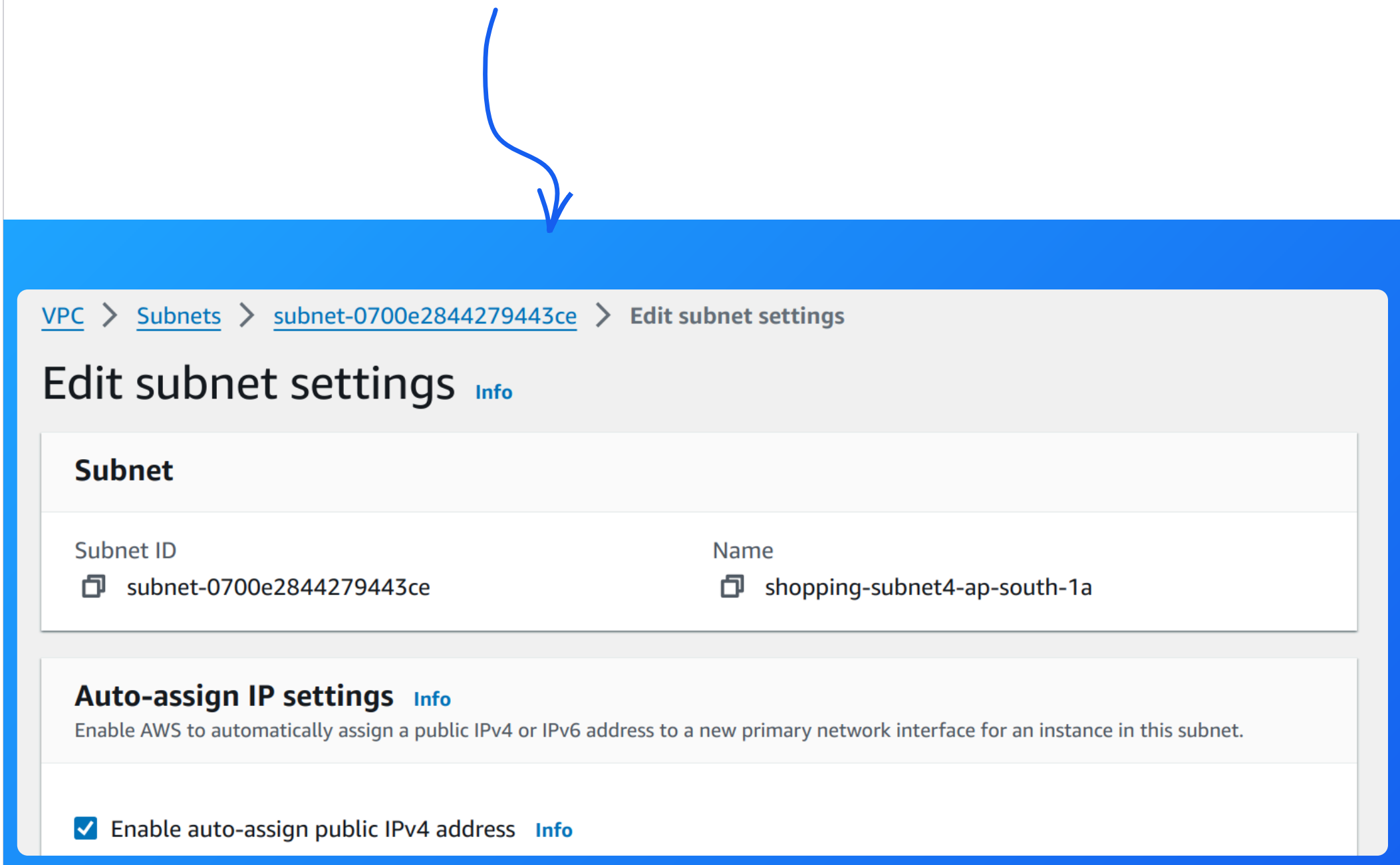
Anitta Philip
https://www.linkedin.com/in/anittap/

Enable auto-assign public IPv4 address

When you enable auto-assign public IPv4 address for a subnet, any EC2 instance launched in that subnet will automatically receive a public IP address. This makes the instance accessible from the internet without needing to manually assign a public IP.

To attach Enable auto-assign public IPv4 address:

- Right-click the subnet
- Select edit subnet settings
- Enable auto-assign public IPv4 address



Anitta Philip
https://www.linkedin.com/in/anittap/

NextWork.org

Update Route Tables

A route table in AWS defines rules that determine where network traffic from instances within a VPC is directed. It maps destination IP addresses to specific destinations, such as other subnets within the VPC, virtual private gateways, or internet gateways. By configuring route tables, you control how network traffic flows between different parts of your VPC and external networks like the internet.

- After attaching the IGW, update the route tables associated with your VPC.
- Edit the route table that your public-facing subnets use.
- Add a route (0.0.0.0/0) pointing to the newly attached IGW. This tells your VPC how to route internet-bound traffic.


Anitta Philip
https://www.linkedin.com/in/anittap/

My key learnings

1. If AWS didn’t have VPCs, the organization and security of resources would be less granular and more challenging to manage. Networks would be less isolated, potentially exposing resources to broader risks and making it harder to control access and traffic flow. Security configurations would likely need to rely more on traditional firewall setups rather than the flexible, policy-driven controls that VPCs provide.

2. A CIDR block is a method for specifying IP addresses and their associated routing prefixes. It allows networks to be divided into smaller, more manageable subnetworks, each identified by a unique CIDR notation that combines an IP address and a prefix length indicating the network's size.

3. The difference between a public and a private subnet lies in their accessibility and routing configuration. A public subnet has a route to an Internet Gateway (IGW) and typically allows instances to have public IP addresses, enabling direct internet access. In contrast, a private subnet does not have a route to an IGW and uses a NAT gateway or NAT instance for outbound internet access, keeping instances within it isolated from direct internet communication.

4. One One thing I didn’t expect was how quickly I could set up and configure a VPC with subnets and an internet gateway on AWS. It was faster and more straightforward than I initially anticipated, especially with the automated features like auto-assigning public IPs and the intuitive AWS Management Console interface.