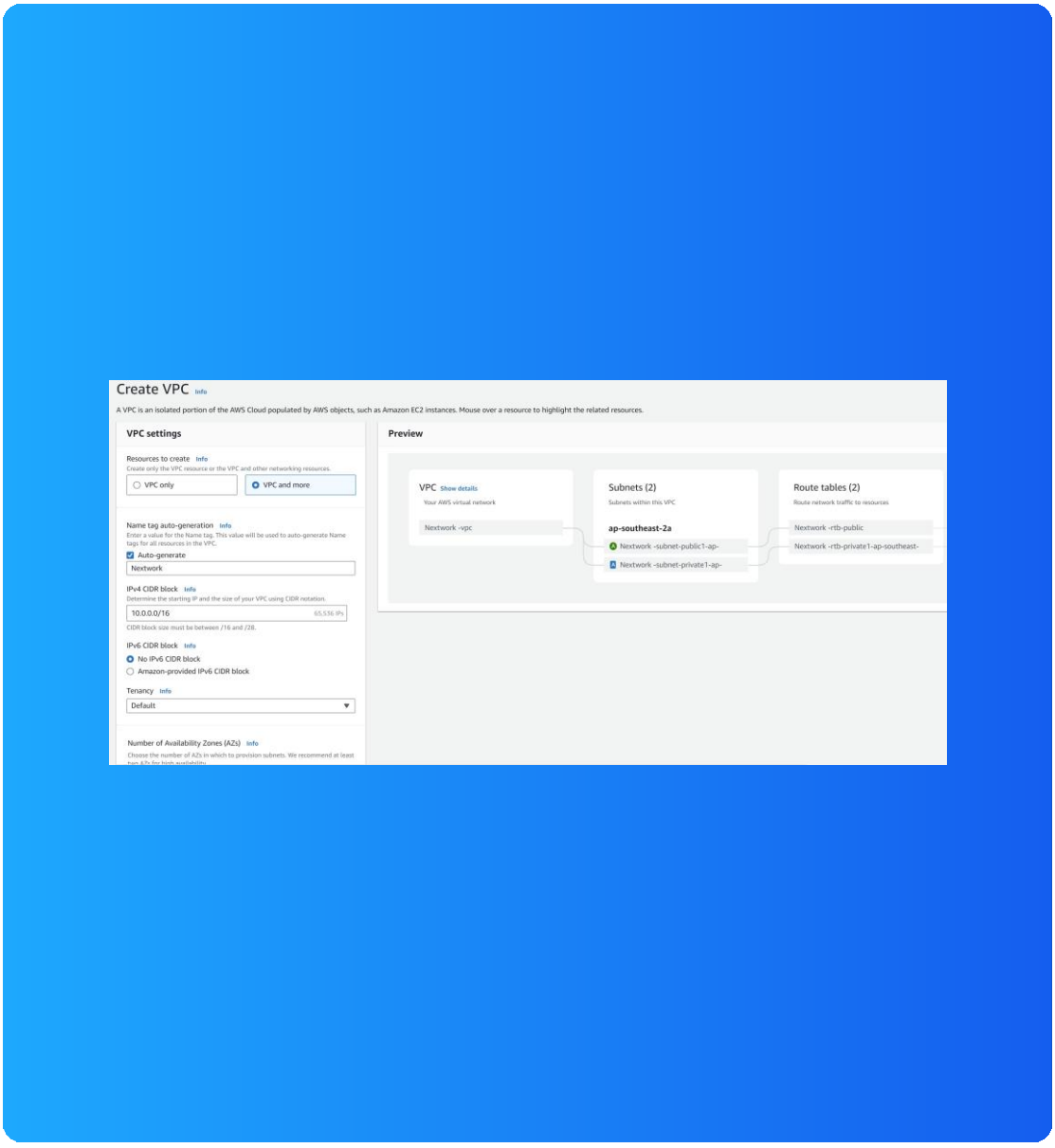
NextWork.org

Launching VPC Resources

https://www.linkedin.com/in/prajit-venkatachalam-435b2a150/

Prajit Venkatachalam



V

Prajit Venkatachalam
https://www.linkedin.com/in/prajit-venkatachalam-435b2a150/

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) exists within an AWS region and is used to build a private and secure connection for resources in the subnets. Through an internet gateway, these resources and users can access internet to communicate each other.

How I used Amazon VPC in this project

I used Amazon VPC to create my own VPC with various resources and components (e.g., security groups and network ACLs), private resources (e.g., a private subnet), and EC2 instances in both my public and private subnets.

One thing I didn't expect in this project was...

One thing I didn't expect was for the resource map to be so visual and interactive. It's such a convenient and quick way to set up an entire VPC architecture.

This project took me...

This project took me 2.5 hours to complete, including the report writing.

V

Prajit Venkatachalam
https://www.linkedin.com/in/prajit-venkatachalam-435b2a150/

Setting Up Direct VM Access

Directly accessing a virtual machine means logging into an EC2 instance (instead of just managing it at a higher level with the AWS Management Console). This includes operations like installing software and changing the EC2 instance's configuration.

SSH is a key method for directly accessing a VM

SSH stands for Secure Shell, and it is both a protocol and a traffic type. It is the protocol that matches key pairs and allows direct VM access, and once the connection is established, the traffic encrypts the communication data being transmitted.

To enable direct access, I set up key pairs

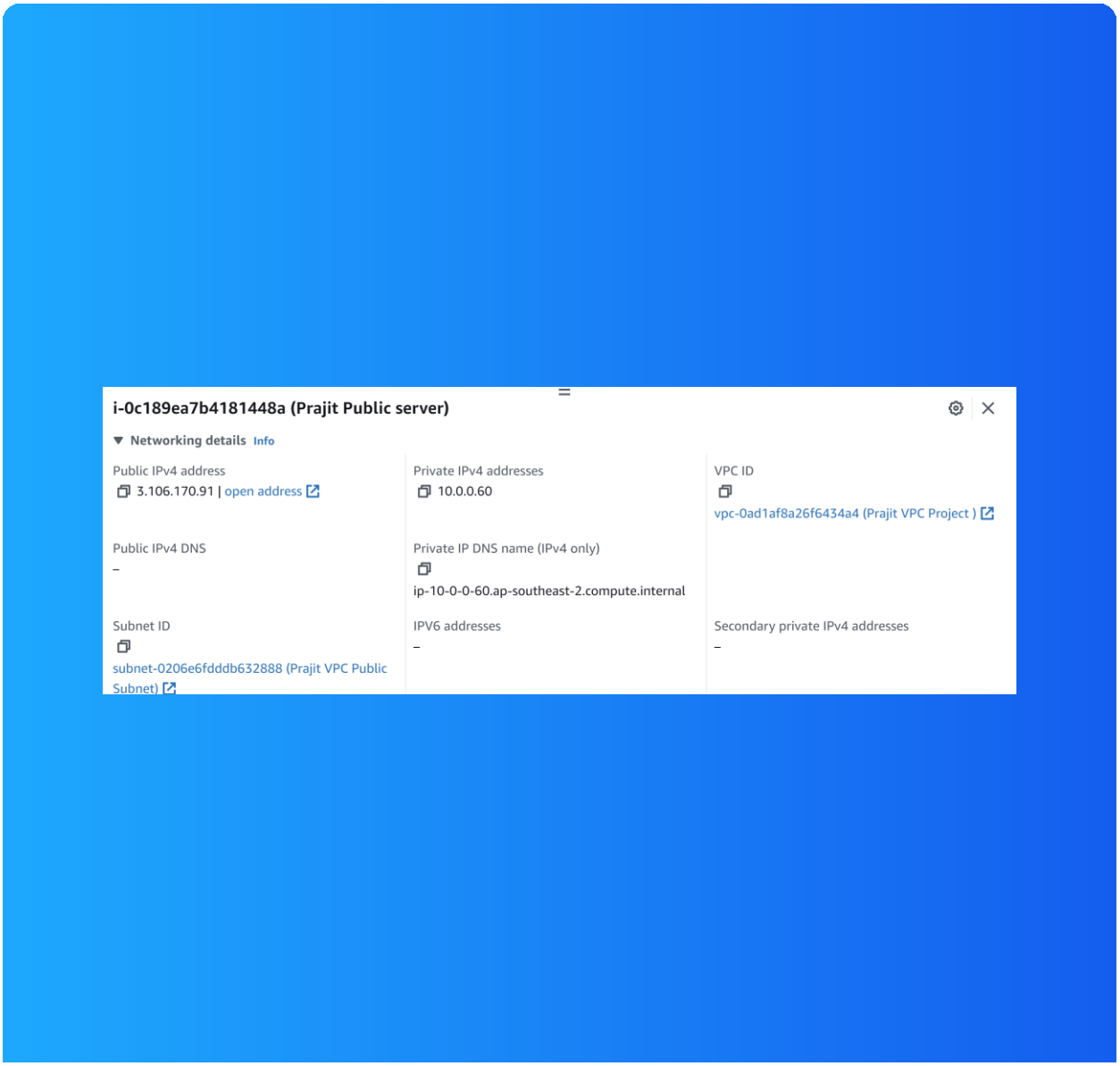
Key pairs are tools that help engineers authenticate themselves when trying to access a virtual machine (EC2 instance). Key pairs work by having two keys—a private key for the VM and a matching public key for the user.

A private key's file format refers to the file type in which the key is stored. My private key's file format was .pem, which is a widely accepted format that most servers can read or use.

Prajit Venkatachalam
https://www.linkedin.com/in/prajit-venkatachalam-435b2a150/

Launching a public server

I had to change my EC2 instance's networking settings by changing the VPC and subnet in which it was going to be launched. I updated both to my Prajit VPC and public subnet, respectively, and used my existing public security group.

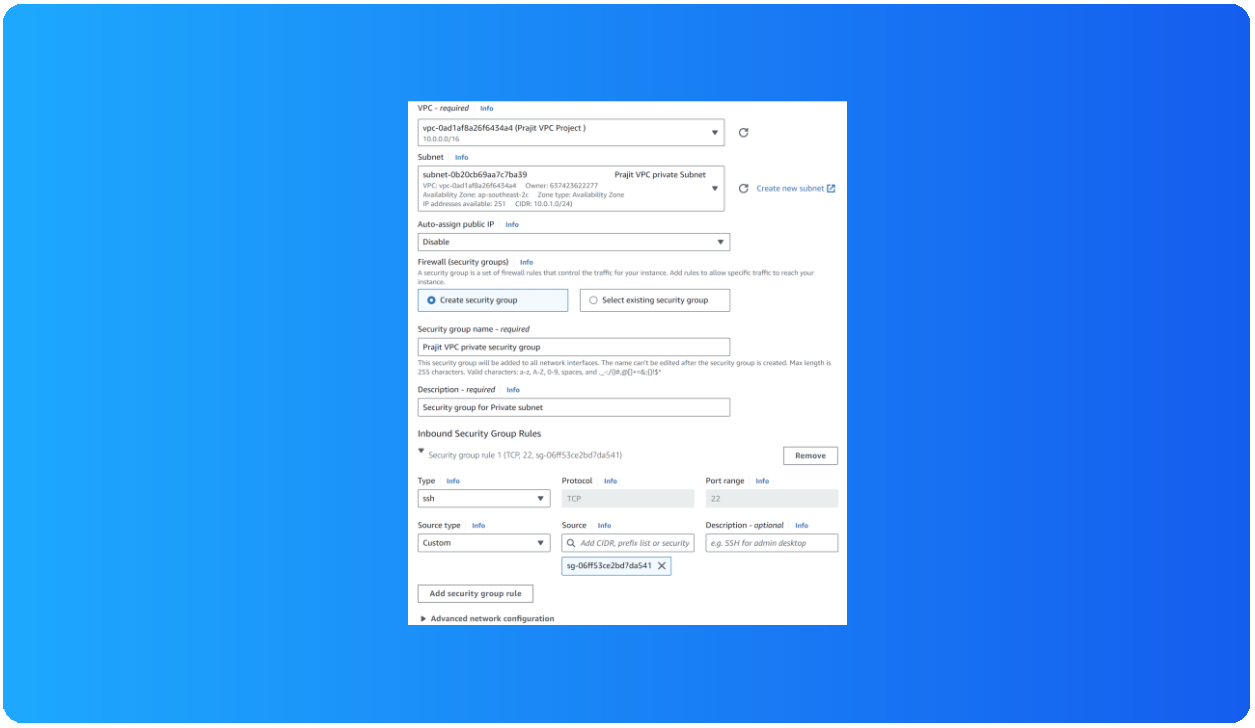


Prajit Venkatachalam
https://www.linkedin.com/in/prajit-venkatachalam-435b2a150/

Launching a private server

My private server has its own dedicated security group because the 'Prajit VPC public security group' allows in all HTTP traffic, which would make the private server more vulnerable to security attacks and risks.

The source of my private server's security group is my 'Prajit VPC public security group', which means only SSH traffic originating from resources associated with that security group (Prajit VPC public security group) is allowed.



V

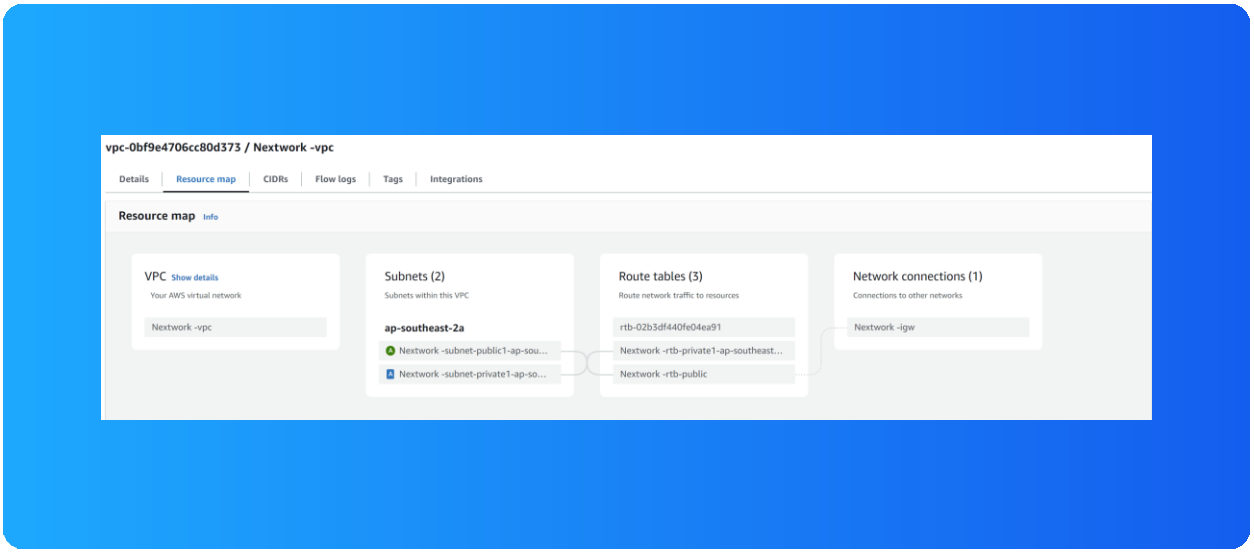
Prajit Venkatachalam
https://www.linkedin.com/in/prajit-venkatachalam-435b2a150/

Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I selected the 'VPC and more' option, which provides a resource map to guide the creation of the VPC and its components, such as security groups, route tables, and internet gateways.

A VPC resource map is a visual diagram that outlines my VPC's components and the relationships or connections between them. The resource map is interactive; it highlights the connections relevant to any resource that I select.

My new VPC has a CIDR block of 10.0.0.0/16. It is possible for it to have the same IPv4 CIDR block as my existing VPC because VPCs are inherently isolated from each other. However, this is not best practice, especially if VPC peering is needed.



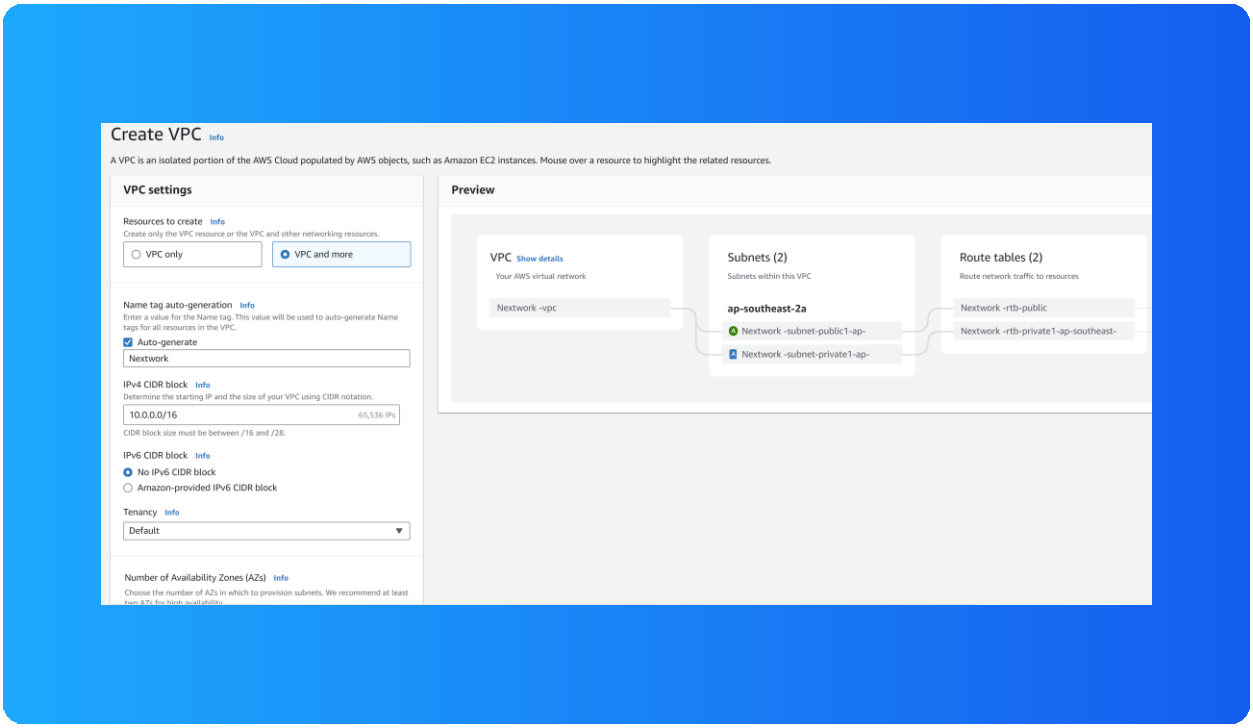
Prajit Venkatachalam
https://www.linkedin.com/in/prajit-venkatachalam-435b2a150/

Speeding up VPC creation

Tips for using the VPC resource map

When determining the number of public subnets in my VPC, I only had two options: either none or one in each availability zone. This is because it is best practice (to improve redundancy and high availability) to have at least one subnet per AZ.

The setup page also offered to create NAT gateways, which are connector gateways that allow resources in my private subnet to access the internet (e.g., for security updates) while still blocking incoming traffic from the internet.



Everyone should be in a job they love.

Check out nextwork.org for more projects