



Launching VPC Resources

J

Michael K.

The screenshot shows the 'Create VPC' wizard in the AWS VPC console. On the left, the configuration pane includes:

- Name tag auto-generation**: A dropdown menu with 'Auto-generate' selected, showing the tag 'vpc-resource-map-test'.
- IPv4 CIDR block**: Set to '10.0.0.0/16'.
- IPv6 CIDR block**: Set to 'No IPv6 CIDR Block'.
- Tenancy**: Set to 'Default'.
- Number of Availability Zones (AZs)**: Set to '3'.
- Customize AZs**: Shows 'use1-az1 (us-east-1a)' as the first availability zone.

On the right, the 'Preview' pane shows the network structure:

- VPC Show details**: Your AWS virtual network.
- Subnets (6)**: Subnets within this VPC:
 - us-east-1a: vpc-resource-map-test-subnet-1, vpc-resource-map-test-subnet-2, vpc-resource-map-test-subnet-3, vpc-resource-map-test-subnet-4, vpc-resource-map-test-subnet-5, vpc-resource-map-test-subnet-6
 - us-east-1b: vpc-resource-map-test-subnet-7, vpc-resource-map-test-subnet-8, vpc-resource-map-test-subnet-9, vpc-resource-map-test-subnet-10, vpc-resource-map-test-subnet-11, vpc-resource-map-test-subnet-12
- Route tables (5)**: Route network traffic to resources:
 - vpc-resource-map-test-rb-public
 - vpc-resource-map-test-rb-private1-us
 - vpc-resource-map-test-rb-private2-us
 - vpc-resource-map-test-rb-private3-us
 - vpc-resource-map-test-rb-private4-us



Michael K.

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a logically isolated virtual network within AWS where I can launch and manage AWS resources (such as EC2 instances, RDS databases, and load balancers) using my own defined IP address range, subnets, route tables, and network gateways.

How I used Amazon VPC in this project

In today's project, I used my already created Amazon VPC and added a resource (server) in each of the subnets (private and public subnet).

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

One thing I didn't expect in this project was the possibility of creating a VPC and its resources in a faster and more simpler way.

This project took me...

This project took me an hour.

Setting Up Direct VM Access

Directly accessing a virtual machine means logging into and managing the operating system or software of the machine as if i was using it in front of me, but over the internet.

SSH is a key method for directly accessing a VM

SSH is the protocol used for a secure access to a remote machine. When i connect to the instance, SSH verifies i possess the correct private key corresponding to the public key on the server, ensuring only authorized users can access the instance. Once SSH has established a secure connection between me and the EC2 instance, SSH traffic is then used to transmits all data (including my commands and the responses from the instance) encrypted. This encryption makes SSH an ideal method for securely exchanging confidential data e.g. login credentials!

To enable direct access, I set up key pairs

Key pairs are cryptographic keys: one private and one public. The public key is installed on the virtual machine, and the private key remains with the user. When i attempt to connect, the machine uses the public key to create an encrypted challenge that can only be decrypted with the private key. Key pairs make sure that access to my EC2 instances is secure and authenticated.



J

Michael K.

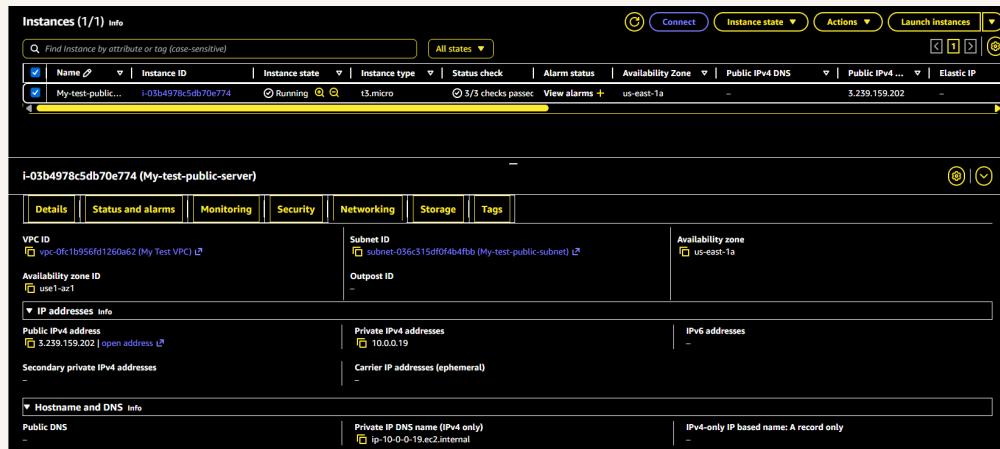
NextWork Student

nextwork.org

A private key's file format is a form in which a private key can be created suited to be procesed by some particular systems or applications. My private Key was in the Privacy Enhanced Mail (.pem) format.

Launching a public server

I had to change my EC2 instance's networking settings by changing the VPC, Subnet and Security settings and using the ones i created earlier.



Launching a private server

My private server has its own dedicated security group because it is designed to only accept traffics from any resource that uses the public security group and wants to access it .

My private server's security group's source is the public security group used by the public server.

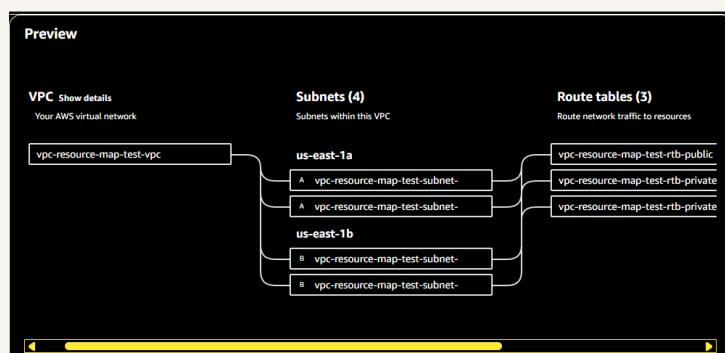
The screenshot shows the AWS EC2 'Launch an instance' wizard, specifically the 'Configure Instance Details' step. The user is creating a new security group named 'test-private-server-security-group'. The 'Description' field contains 'Security group for private test subnet.' Under 'Inbound Security Group Rules', there is one rule defined: 'Security group rule 1 (TCP, 22, sg-01118d6fb1891797a)'. This rule allows TCP traffic on port 22 from the security group 'sg-01118d6fb1891797a'. The 'Source type' dropdown is set to 'Custom', and the 'Source' dropdown lists the security group 'sg-01118d6fb1891797a'. There are 'Add security group rule' and 'Advanced network configuration' buttons at the bottom of the rule section.

Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I used VPC Resource Map.

A VPC resource map is a tool to quickly understand the architectural layout of a VPC, like the number of subnets, which subnets are associated with which route table, and which route tables have routes to an internet gateway.

My new VPC has a CIDR block of 10.0.0.0/16. It is possible for my new VPC to have the same IPv4 CIDR block as my existing VPC because VPCs in a region are totally isolated from each other hence preventing any IP Address overlap.

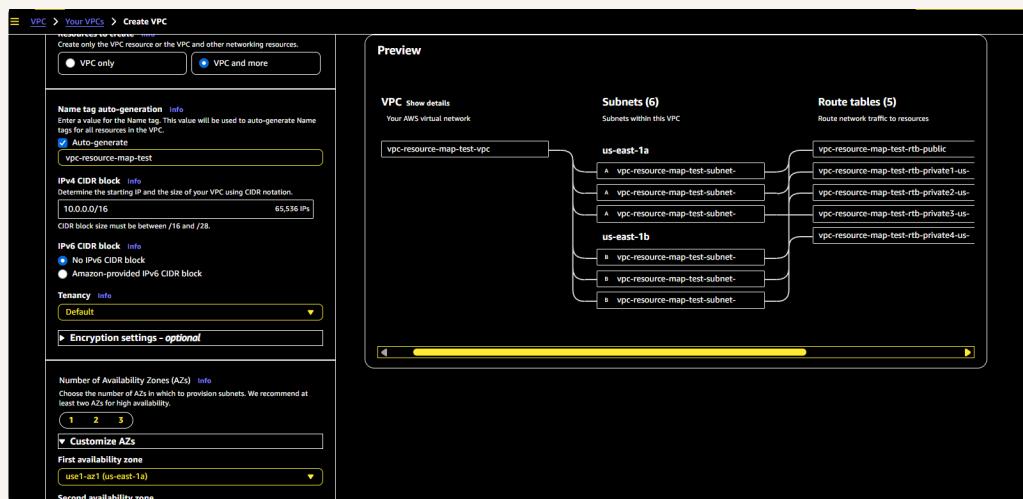


Speeding up VPC creation

Tips for using the VPC resource map

When determining the number of public subnets in my VPC, I only had two options: 0 or 2. This was because i had chosen 2 AZ. Having chosen 2 public Subnets to create, the Wizards interprets that choice of AZ and Subnet number as a way to setup a redundant and high available system with a backup subset.

The set up page also offered to create NAT gateways, which let instances in private subnets access the internet for updates and patches, while blocking inbound traffic.





nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

