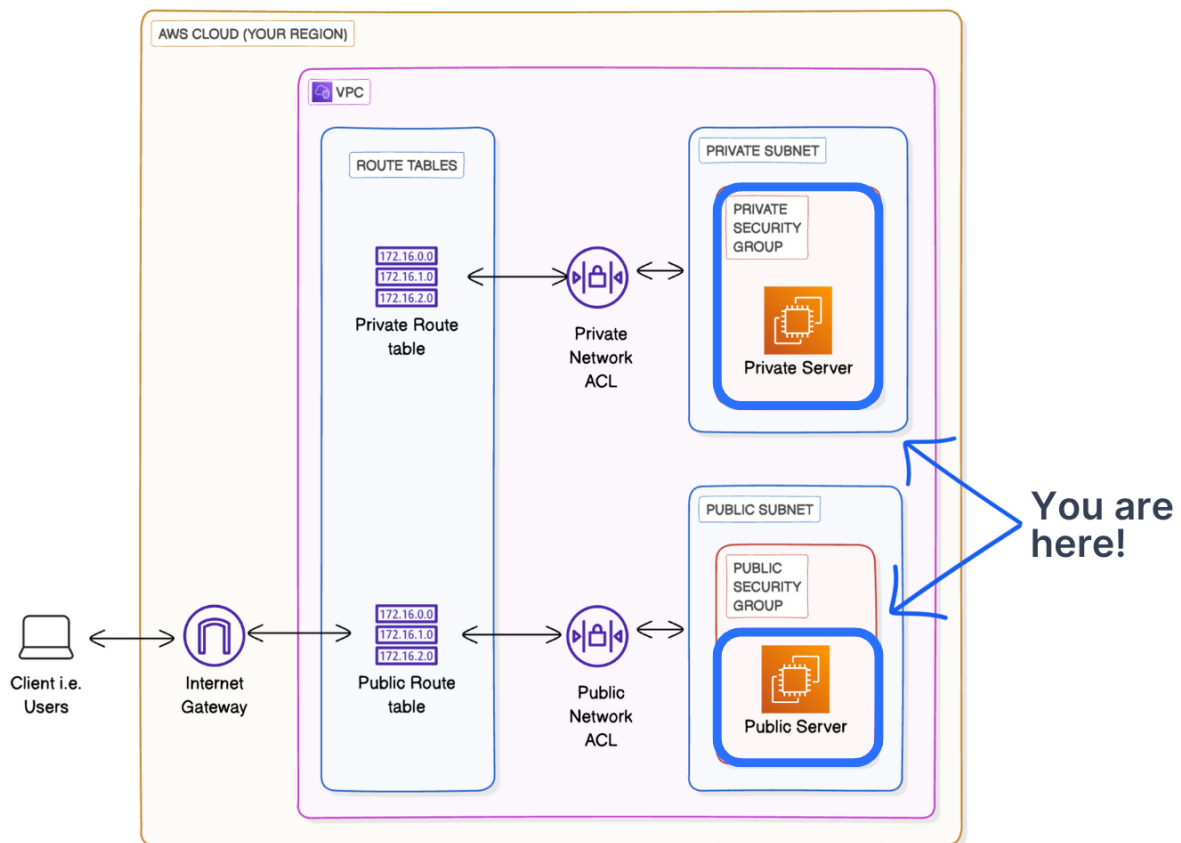


Launching VPC Resources



Launch a Public EC2 Instance

Head to the **EC2 console** - search for EC2 in the search bar at the top of screen.

Select **Instances** at the left hand navigation bar.

- Select **Launch instances**.
- Since your first EC2 instance will be launched in the public subnet, let's name it NextWork Public Server
- For the **Amazon Machine Image**, select **Amazon Linux 2023 AMI**.
- For the **Instance type**, select **t2.micro**.
- For the **Key pair (login)** panel, select **Create new key pair**.
- For the **Key pair name**, use NextWork key pair
- Keep the **Key pair type** as **RSA**, and the **Private key file format** as **.pem**
- Select **Create key pair**.
- At the **Network settings** panel, select **Edit** at the right-hand corner.
- Select **NextWork VPC** from the drop-down in the VPC list.
- Select your public subnet.
- For the **Firewall (security groups)**, we've already created the security group for your public subnet's resources. Choose **Select existing security group**.
- Select **NextWork Public Security Group**.
- Select **Launch instance**.

- Click into your instance once it's successfully launched.
- Head back to the **Instances** page.
- Select the checkbox next to your instance, and a **Details** panel pops up
- Switch the tab to **Networking**.
- Notice how your public server has a Public IPv4 address, a subnet it's associated with, an Availability zone it's launched in, and a VPC ID that links it with NextWork VPC too.

The screenshot shows the 'Launch an instance' page in the AWS Management Console. The 'Networking' tab is selected, showing the following settings:

- VPC - required:** vpc-038bbba68b4dbf4d (NextWork VPC)
- Subnet:** subnet-08cf7637b8146a1a7 (Public 1)
- Auto-assign public IP:** Enable
- Firewall (security groups):** Select existing security group (NextWork Security Group - sg-06e886aa6631cfee)

The 'Summary' panel on the right shows:

- Number of instances:** 1
- Software Image (AMI):** Amazon Linux 2023 AMI 2023.6.2...
- Virtual server type (instance type):** t2.micro
- Firewall (security group):** NextWork Security Group
- Storage (volumes):** 1 volume(s) - 8 GiB

Buttons at the bottom include 'Cancel', 'Launch instance', and 'Preview code'.

Launch a Private EC2 Instance

- Select Launch instances again.
- Name: NextWork Private Server
- Amazon Machine Image (AMI): Amazon Linux 2023 AMI
- Instance type: t2.micro
- Key pair: NextWork key pair
- At the **Network settings** panel, select **Edit** at the right hand corner.
- Network: **NextWork VPC**
- Subnet: **NextWork Private Subnet**
- **Firewall (security groups):** we said we'd use an alternative way to set up security groups for your private subnet's resources, and here we are!
 - Select **Create security group**.
 - For **Security group name**, let's use NextWork Private Security Group
 - For Description, we'll replace the default value with Security group for NextWork Private Subnet.
 - Notice the default Inbound Security Groups, the **Type** is set to **ssh**.
- Change the **Source type** from **Anywhere** to **Custom**.
- In the **Source** drop down, scroll down and select **NextWork Public Security Group**.
- Select **Launch instance**.

EC2 > Instances > Launch an instance

Firewall (security groups) | Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - *required*
NextWork Private Security Group

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&{}!\$*

Description - *required* | Info
Security group for NextWork Private Subnet.

Inbound Security Group Rules
▼ Security group rule 1 (TCP, 22, sg-06e886aa6631ccfee) Remove

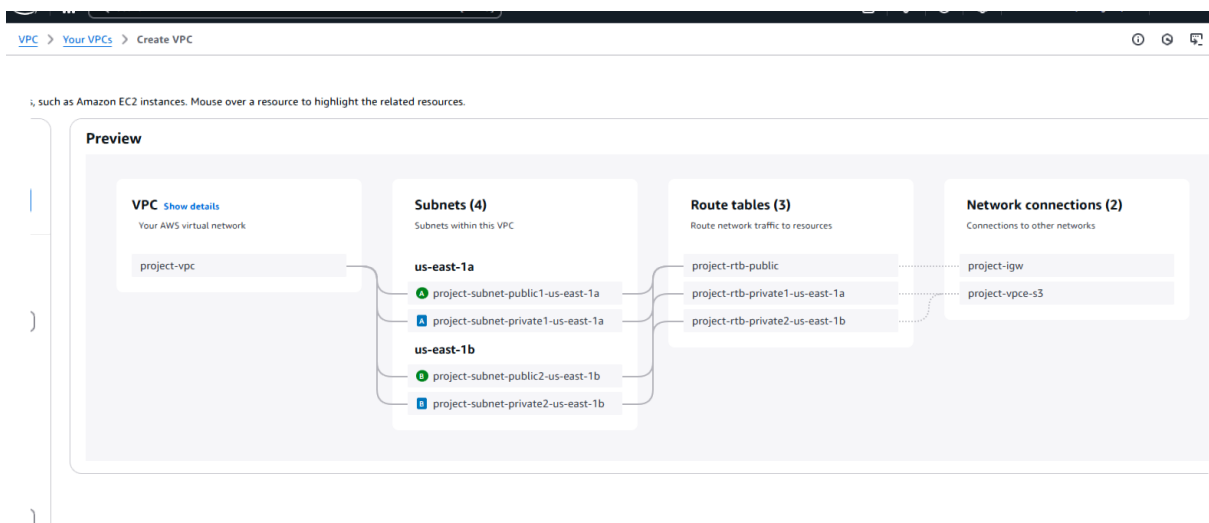
Type	Protocol	Port range	Source type	Source	Description - optional
ssh	TCP	22	Custom	sg-06e886aa6631ccfee	e.g. SSH for admin desktop

Add security group rule

Launch your VPC setup in minutes

In this step, you're going to:

- Try a new way to create your entire VPC setup
- Head back to your VPC console.
- From the left-hand navigation bar, select Your VPCs.
- Select Create VPC.
- We previously stuck to creating a VPC only, but this time select VPC and more.
- A visual flow diagram pops up that shows us other VPC resources. This is called a VPC resource map!





- Scroll back to the left-hand side of the screen to see the VPC's set up.
- Under **Name tag auto-generation**, enter nextwork
- The VPC's **IPv4 CIDR block** is already pre-filled to 10.0.0.0/16
- For **IPv6 CIDR block**, we'll leave in the default option of **No IPv6 CIDR block**.
- For **Tenancy**, we'll keep the selection of **Default**.
- For **Tenancy**, we'll keep the selection of **Default**.
- For **Number of Availability Zones (AZs)**, we'll leave the default value of **2** for now and come back to this soon.
- Expand the **Customize AZs** arrow. You can even configure which two Availability Zones you'd like to set up for this VPC!
- Next, notice that **Number of public subnets** only gives you two options - **0** or **2**.
- Similar to this, **Number of private subnets** only gives you three options - **0**, **2** or **4**.
- Change the **Number of private subnets** from **2** to **1**. Now we have just two subnets total - one public and one private subnet!
- Update your public and private subnets' CIDR blocks:
 - Update your public subnet CIDR block to 10.0.0.0/24
 - Update your private subnet CIDR block to 10.0.1.0/24
- Next, for the **NAT gateways (\$)** option, make sure you've selected **None**. As the dollar sign suggests, NAT gateways cost money!
- Next, for the **VPC endpoints** option, select **None**.
- You can leave the **DNS options** checked.
- Select **Create VPC**.
- Super satisfying to see this loading bar of your VPC and its resources getting created

Create VPC workflow

✔ Success

▼ Details

- ✔ Create VPC: [vpc-01292afd8bd4f29cf](#) 
- ✔ Enable DNS hostnames
- ✔ Enable DNS resolution
- ✔ Verifying VPC creation: [vpc-01292afd8bd4f29cf](#) 
- ✔ Create subnet: [subnet-0777106d4ecb1bd3e](#) 
- ✔ Create subnet: [subnet-028170a17c2b0ed48](#) 
- ✔ Create internet gateway: [igw-05a45a2b6419a5af8](#) 
- ✔ Attach internet gateway to the VPC
- ✔ Create route table: [rtb-02784a4f8cdfc0935](#) 
- ✔ Create route
- ✔ Associate route table
- ✔ Create route table: [rtb-08b551c83b97de8e9](#) 
- ✔ Associate route table
- ✔ Verifying route table creation

-
- Select **View VPC**.
- Select the checkbox next to **nextwork-vpc**.
- Select the **Resource map** tab.
- Now uncheck **nextwork-vpc**, and select your original **NextWork VPC**.
- Select the **Resource map** tab again.
- There's a resource map for VPCs we create from scratch too.

PCs

> vpc-01292afd8bd4f29cf

Available

Off

Enabled

vpcc-01292afd8bd4f29cf

Available

Off

Enabled

DNS resolution

Enabled

Main network ACL

acl-0158c6d7b4a651392

IPv6 CIDR (Network border group)

-

Tenancy

default

Default VPC

No

Network Address Usage metrics

Disabled

DHCP option set

dopt-06565688339babf4f

IPv4 CIDR

10.0.0.0/16

Route 53 Resolver DNS Firewall rule groups

-

Main route table

rtb-044c2b6ece3f34dc7

IPv6 pool

-

Owner ID

329599662468

Resource map

CIDRs

Flow logs

Tags

Integrations

Resource map

Info

VPC

Show details

Your AWS virtual network

nextwork-vpc

Subnets (2)

Subnets within this VPC

us-east-1a

nextwork-subnet-public1-us-east-...

nextwork-subnet-private1-us-east-...

Route tables (3)

Route network traffic to resources

rtb-044c2b6ece3f34dc7

nextwork-rtb-public

nextwork-rtb-private1-us-east-1a

Network connections

Connections to other networks

nextwork-igw

lattice