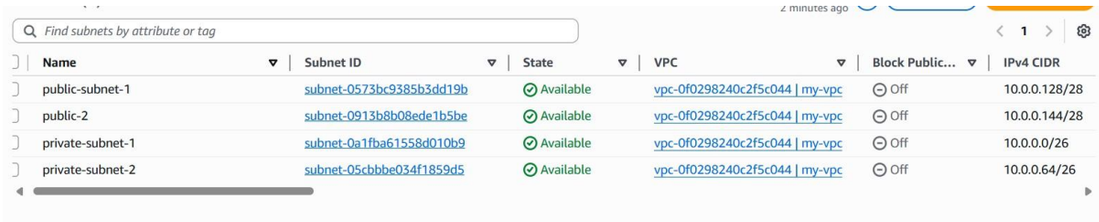
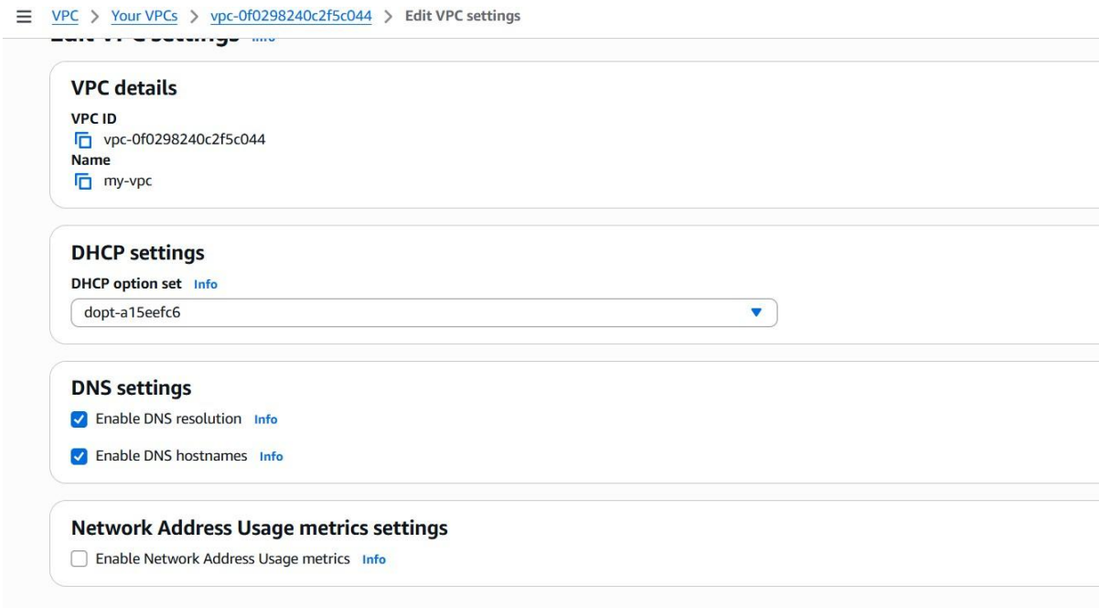
1) Create VPC with 2 private and 2 public subnets.



Find subnets by attribute or tag

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
public-subnet-1	subnet-0573bc9385b3dd19b	Available	vpc-0f0298240c2f5c044 | my-vpc	Off	10.0.0.128/28
public-2	subnet-0913b8b08ede1b5be	Available	vpc-0f0298240c2f5c044 | my-vpc	Off	10.0.0.144/28
private-subnet-1	subnet-0a1fba61558d010b9	Available	vpc-0f0298240c2f5c044 | my-vpc	Off	10.0.0.0/26
private-subnet-2	subnet-05cbbbe034f1859d5	Available	vpc-0f0298240c2f5c044 | my-vpc	Off	10.0.0.64/26

2) Enable DNS Hostname in VPC



VPC > Your VPCs > vpc-0f0298240c2f5c044 > Edit VPC settings

VPC details

VPC ID
vpc-0f0298240c2f5c044
Name
my-vpc

DHCP settings

DHCP option set Info
dopt-a15eefc6

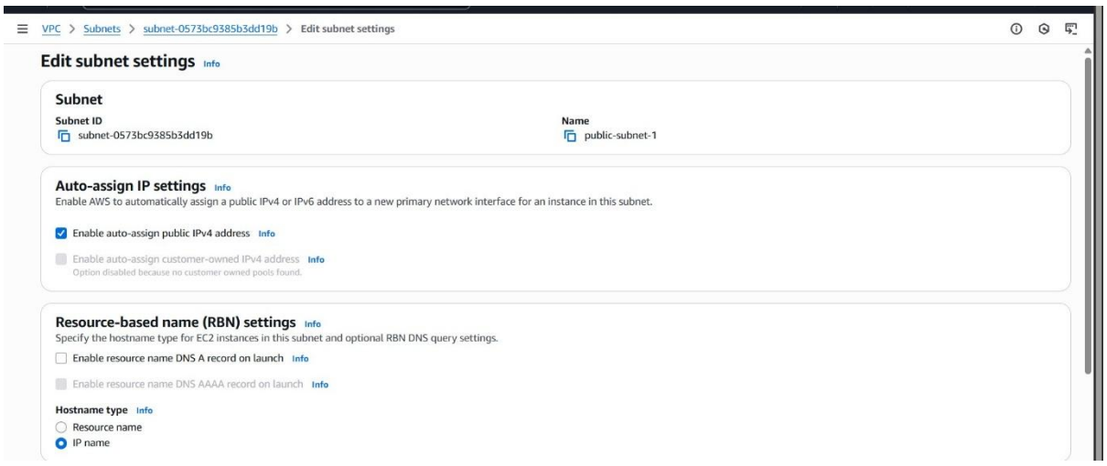
DNS settings

Enable DNS resolution Info
Enable DNS hostnames Info

Network Address Usage metrics settings

Enable Network Address Usage metrics Info

3) Enable Auto Assign Public ip in 2 public subnets



VPC > Subnets > subnet-0573bc9385b3dd19b > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID
subnet-0573bc9385b3dd19b
Name
public-subnet-1

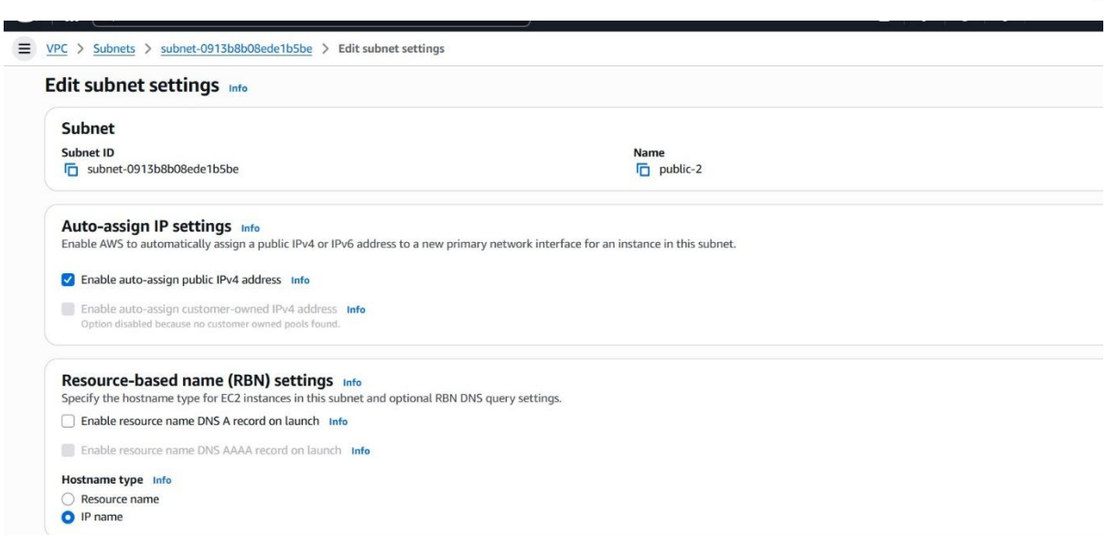
Auto-assign IP settings Info
Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

Enable auto-assign public IPv4 address Info
Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info
Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch Info
Enable resource name DNS AAAA record on launch Info

Hostname type Info
Resource name
IP name



VPC > Subnets > subnet-0913b8b08ede1b5be > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID
subnet-0913b8b08ede1b5be
Name
public-2

Auto-assign IP settings Info
Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

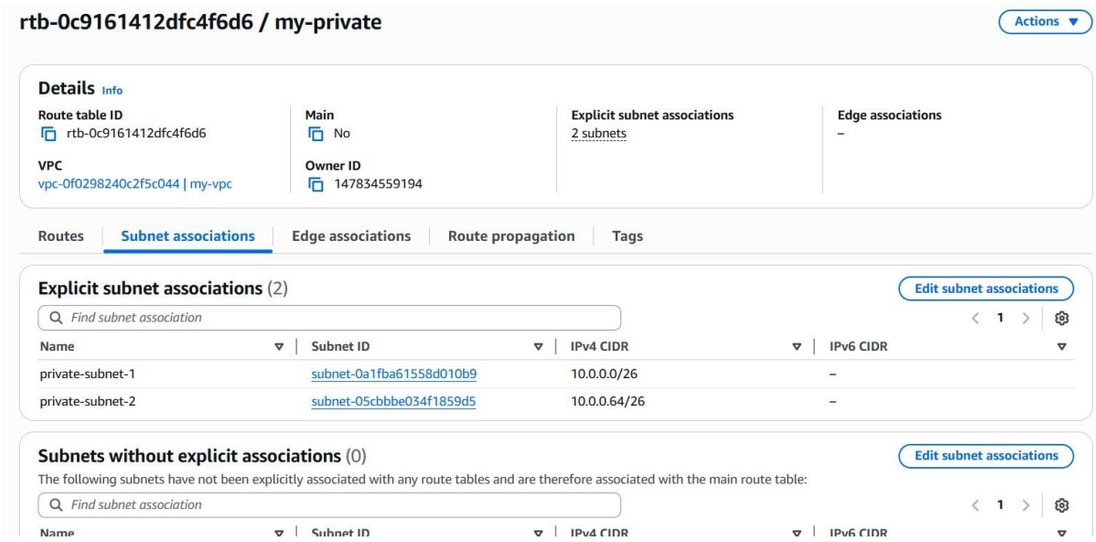
Enable auto-assign public IPv4 address Info
Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info
Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

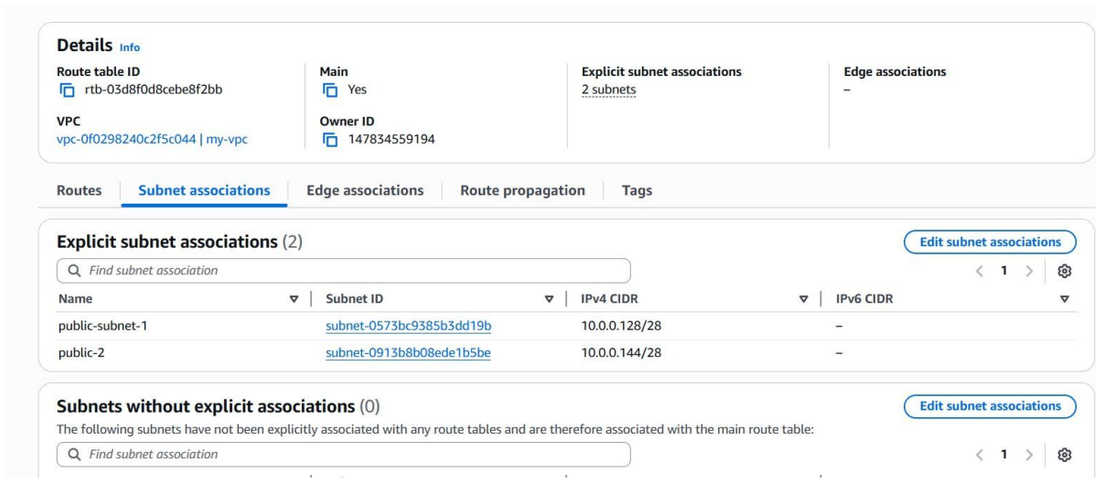
Enable resource name DNS A record on launch Info
Enable resource name DNS AAAA record on launch Info

Hostname type Info
Resource name
IP name

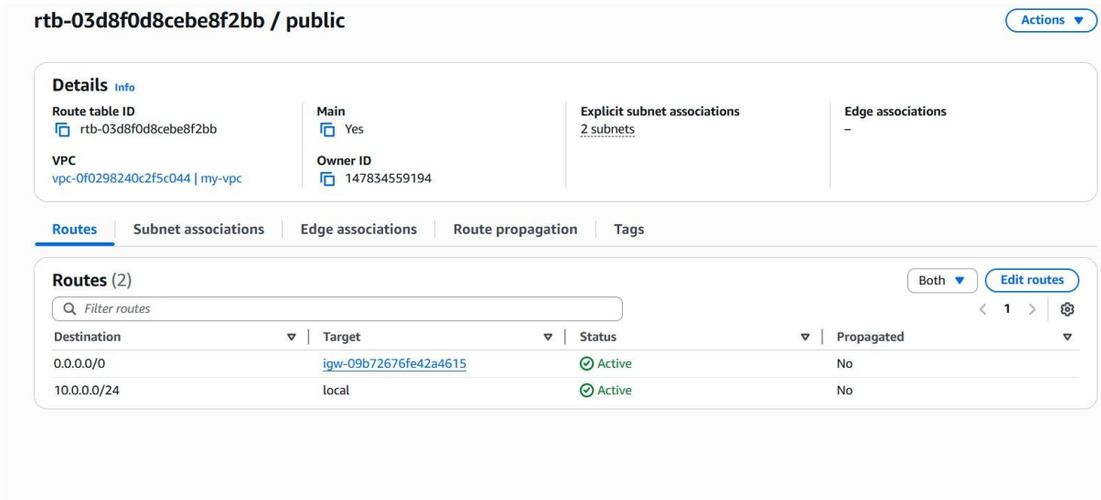
4) Add 2 private subnets in private route table



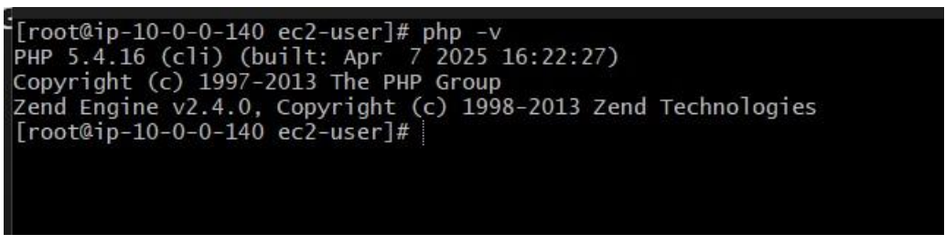
5) Add 2 public subnets in public route table



6) Public route table will have the routes to internet and local



7) Create Ec2 in public subnet with t2micro and install php



8) COnfigure Nat gateway in public subnet and connect to private Instance

Configured nat gateway in public subnet and connected to private instance

Public machine 10.0.0.140 for this machine logged in to 10.0.0.7 private machine and from that private machine pinging google.com

```
[ec2-user@ip-10-0-0-140 ~]$ ssh -i key.pem ec2-user@10.0.0.7
Last login: Mon Jun  9 12:20:39 2025 from ip-10-0-0-140.us-west-2.compute.internal
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2026-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-0-7 ~]$ ping google.com
PING google.com (142.251.215.238) 56(84) bytes of data.
64 bytes from sea09s35-in-f14.1e100.net (142.251.215.238): icmp_seq=1 ttl=116 time=7.84 ms
64 bytes from sea09s35-in-f14.1e100.net (142.251.215.238): icmp_seq=2 ttl=116 time=6.58 ms
64 bytes from sea09s35-in-f14.1e100.net (142.251.215.238): icmp_seq=3 ttl=116 time=6.99 ms
64 bytes from sea09s35-in-f14.1e100.net (142.251.215.238): icmp_seq=4 ttl=116 time=7.52 ms
AC
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 6.582/7.237/7.846/0.493 ms
[ec2-user@ip-10-0-0-7 ~]$
```

9) Install Apache Tomcat in private ec2 and deploy a sample app.

```
[root@ip-10-0-0-7 tomcat]# cd webapps/
[root@ip-10-0-0-7 webapps]# wget https://tomcat.apache.org/tomcat-9.0-doc/appdev
/sample/sample.war
--2025-06-09 12:47:50--  https://tomcat.apache.org/tomcat-9.0-doc/appdev/sample/
sample.war
Resolving tomcat.apache.org (tomcat.apache.org)... 151.101.2.132, 2a04:4e42::644
Connecting to tomcat.apache.org (tomcat.apache.org)|151.101.2.132|:443... connec
ted.
HTTP request sent, awaiting response... 200 OK
Length: 4606 (4.5K)
Saving to: 'sample.war'

100%[======================================>] 4,606       --.-K/s   in 0s

2025-06-09 12:47:50 (30.0 MB/s) - 'sample.war' saved [4606/4606]

[root@ip-10-0-0-7 webapps]# ls
docs  examples  host-manager  manager  ROOT  sample.war
[root@ip-10-0-0-7 webapps]# ls
docs  examples  host-manager  manager  ROOT  sample  sample.war
[root@ip-10-0-0-7 webapps]# ls
docs  examples  host-manager  manager  ROOT  sample  sample.war
[root@ip-10-0-0-7 webapps]# clear
[root@ip-10-0-0-7 webapps]# curl http://localhost:8080/sample/
<html>
<head>
<title>Sample "Hello, World" Application</title>
</head>
<body bgcolor=white>

<table border="0">
<tr>
<td>
<img src="images/tomcat.gif">
</td>
<td>
<h1>Sample "Hello, World" Application</h1>
<p>This is the home page for a sample application used to illustrate the
source directory organization of a web application utilizing the principles
outlined in the Application Developer's Guide.
</td>
</tr>
</table>

<p>To prove that they work, you can execute either of the following links:
<ul>
<li>To a <a href="hello.jsp">JSP page</a>.
<li>To a <a href="hello">servlet</a>.
</ul>

</body>
</html>
[root@ip-10-0-0-7 webapps]#
```

10) Configure VPC flow logs and store the logs in s3 and cloudwatch.