

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

The screenshot shows the 'Your VPCs (1/2)' page in the AWS Management Console. A table lists two VPCs: one unnamed with ID `vpc-094bc96058326e6e0` and CIDR `172.31.0.0/16`, and another named 'myvpc' with ID `vpc-03f8a2ff2fc5f8333` and CIDR `191.50.0.0/16`. Below the table, a diagram illustrates the network architecture for the 'myvpc' VPC. It shows a central box for 'Subnets within this VPC' in the `us-east-1a` region, containing four subnets: `pub1_subnet`, `pub2_subnet`, `priv1_subnet`, and `priv2_subnet`. To the left, a box labeled 'Your AWS virtual network' contains the 'myvpc' VPC. To the right, a box labeled 'Route network traffic to resources' shows a route table `rtb-028f40195c97d2690` with lines connecting it to the public subnets.

2) Enable DNS Hostname in VPC.

The screenshot shows the 'Edit VPC settings' page for VPC `vpc-03f8a2ff2fc5f8333`. The breadcrumb trail is `VPC > Your VPCs > vpc-03f8a2ff2fc5f8333 > Edit VPC settings`. The page is divided into three sections: 'VPC details', 'DHCP settings', and 'DNS settings'. The 'VPC details' section shows the VPC ID `vpc-03f8a2ff2fc5f8333` and the name 'myvpc'. The 'DHCP settings' section shows the 'DHCP option set' as `dopt-0ece5646ae242f25d`. The 'DNS settings' section has two checkboxes: 'Enable DNS resolution' and 'Enable DNS hostnames', both of which are checked.

3) Enable Auto Assign Public IP in 2 public subnets

VPC > Subnets > subnet-0ab3340c6d96c23a7 > Edit subnet settings

Edit subnet settings [Info](#)

Subnet
Subnet ID
 subnet-0ab3340c6d96c23a7

Name
 pub1_subnet

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](#)

VPC > Subnets > subnet-06422208dd11b1af0 > Edit subnet settings

Edit subnet settings [Info](#)

Subnet
Subnet ID
 subnet-06422208dd11b1af0

Name
 pub2_subnet

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](#)

4) Add 2 private subnets in private route table

Route tables (1/4) [Info](#) Last updated 3 minutes ago [Actions](#) [Create route table](#)

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VF
<input type="checkbox"/>	-	rtb-05dec867bcc1d6fc	-	-	Yes	vp
<input type="checkbox"/>	my_route	rtb-05a6271b49fc49a46	2 subnets	-	No	vp
<input type="checkbox"/>	-	rtb-028f40195c97d2690	-	-	Yes	vp
<input checked="" type="checkbox"/>	my_route2	rtb-03bc5821874d330d7	2 subnets	-	No	vp

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
priv1_subnet	subnet-0104b1d41f2d46fba	191.50.2.128/25	-
priv2_subnet	subnet-0217246abca2b515e	191.50.3.192/26	-

5) Add 2 public subnets in public route table

Route tables (1/4) Info

Last updated 2 minutes ago

Actions

Create route table

< 1 > ⚙️

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	Vf
<input type="checkbox"/>	-	rtb-05dec867bccf1d6fc	-	-	Yes	vp
<input checked="" type="checkbox"/>	my_route	rtb-05a6271b49fc49a46	2 subnets	-	No	vp
<input type="checkbox"/>	-	rtb-028f40195c97d2690	-	-	Yes	vp

Explicit subnet associations (2)

Edit subnet associations

< 1 > ⚙️

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
pub1_subnet	subnet-0ab3340c6d96c23a7	191.50.0.0/24	-
pub2_subnet	subnet-06422208dd11b1af0	191.50.1.0/24	-

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

rtb-05a6271b49fc49a46

Updated routes for rtb-05a6271b49fc49a46 / my_route successfully

Details

Details Info

Route table ID

[rtb-05a6271b49fc49a46](#)

Main

☒ No

Explicit subnet associations

[2 subnets](#)

Edge associations

-

VPC

[vpc-03f8a2ff2fc5f8333](#) | myvpc

Owner ID

[866018956544](#)

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both

Edit routes

< 1 > ⚙️

Destination	Target	Status	Propagated
0.0.0.0/0	igw-016de0d15415d7c44	Active	No
191.50.0.0/16	local	Active	No

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

Instance summary for i-04600a78532ed1ac5 (my_instance) Info

Updated less than a minute ago

Instance ID

i-04600a78532ed1ac5

Public IPv4 address

3.87.216.198 | [open address](#)

Private IPv4 addresses

191.50.0.91

IPv6 address

—

Instance state

Running

Public DNS

—

Hostname type

IP name: ip-191-50-0-91.ec2.internal

Private IP DNS name (IPv4 only)

ip-191-50-0-91.ec2.internal

Elastic IP addresses

—

Answer private resource DNS name

—

Instance type

t2.micro

AWS Compute Optimizer finding

Opt-in to AWS Compute Optimizer for recommendations. [Learn more](#)

Auto-assigned IP address

3.87.216.198 [Public IP]

VPC ID

vpc-03f8a2ff2fc5f8333 (myvpc) [link](#)

Auto Scaling Group name

—

IAM Role

—

Subnet ID

subnet-0ab3340c6d96c23a7

```

PC@DESKTOP-62H0QCN MINGW64 ~/Downloads
$ ssh -i techie.pem ec2-user@3.87.216.198
The authenticity of host '3.87.216.198 (3.87.216.198)' can't be established.
ED25519 key fingerprint is SHA256:H3v7f6iL82/B6OX3kP5ijDtkA+axbwm0R71BwkkS52c.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.87.216.198' (ED25519) to the list of known hosts.

#_
_###_      Amazon Linux 2
_###_
_###_      AL2 End of Life is 2026-06-30.
_###_
_###_      A newer version of Amazon Linux is available!
_###_      Amazon Linux 2023, GA and supported until 2028-03-15.
_###_      https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-191-50-0-91 ~]$ yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
You need to be root to perform this command.
[ec2-user@ip-191-50-0-91 ~]$ sudo -i
[root@ip-191-50-0-91 ~]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No packages marked for update
[root@ip-191-50-0-91 ~]# yum install php
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                | 3.6 kB      00:00
Resolving Dependencies
--> Running transaction check
--> Package php.x86_64 0:5.4.16-46.amzn2.0.6 will be installed
--> Processing Dependency: httpd-mm = 20120211x8664 for package: php-5.4.16-46.amzn2.0.6.x86_64

```

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

root@ip-191-50-0-194:/home/ec2-user

```
PC@DESKTOP-8IM0QCN MINGW64 ~/Downloads
$ ssh -i "sushma.pem" ec2-user@13.220.213.105
The authenticity of host '13.220.213.105 (13.220.213.105)' can't be established.
ED25519 key fingerprint is SHA256:RBvVXDYtsGLKjvKvNVtOEiLZf9T49wBBuaGUBhTo5PY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.220.213.105' (ED25519) to the list of known hosts.

      #_
     _/  #####_      Amazon Linux 2
    ~~~ \#####\
    ~~~  \###|
    ~~~   \#/
    ~~~    V~' '->
           /
    ~~~  /
    ~~~ /
    ~~~/_/
    ~~~/_/

      A newer version of Amazon Linux is available!

      Amazon Linux 2023, GA and supported until 2028-03-15.
      https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-191-50-0-194 ~]$ sudo su
[root@ip-191-50-0-194 ec2-user]# vi test.pem
[root@ip-191-50-0-194 ec2-user]# ssh -i test.pem ec2-user@191.50.2.135
The authenticity of host '191.50.2.135 (191.50.2.135)' can't be established.
ECDSA key fingerprint is SHA256:Wg3MNufM70sPWKu5Sj+mQswNgIELI4kHIZLlo5uXuwg.
ECDSA key fingerprint is MD5:3e:c0:5f:62:17:fe:a7:96:76:69:89:31:46:66:10:0a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '191.50.2.135' (ECDSA) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'test.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "test.pem": bad permissions
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[root@ip-191-50-0-194 ec2-user]# ping google.com
PING google.com (142.250.31.101) 56(84) bytes of data:
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=1 ttl=108 time=1.39 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=2 ttl=108 time=1.58 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=3 ttl=108 time=1.01 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=4 ttl=108 time=2.00 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=5 ttl=108 time=1.21 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=6 ttl=108 time=1.37 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=7 ttl=108 time=1.25 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 1.014/1.406/2.007/0.296 ms
root@ip-191-50-0-194 ec2-user#
```

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

```
root@ip-191-50-0-194:~/tomcat/webapps
[root@ip-191-50-0-194 tomcat]# cd bin
[root@ip-191-50-0-194 bin]# ls
bootstrap.jar  catalina-tasks.xml  commons-daemon.jar  configtest.sh  digest.sh  setclasspath.bat  shutdown.sh  tomcat-juli.jar  tool-wrapper.sh
catalina.bat  ciphers.bat  commons-daemon-native.tar.gz  daemon.sh  makebase.bat  setclasspath.sh  startup.bat  tomcat-native.tar.gz  version.bat
catalina.sh  cyphers.sh  configtest.bat  digest.bat  makebase.sh  shutdown.bat  startup.sh  tool-wrapper.bat  version.sh
[root@ip-191-50-0-194 bin]# bash startup.sh
Using CATALINA_BASE:   /root/tomcat
Using CATALINA_HOME:   /root/tomcat
Using CATALINA_TMPDIR: /root/tomcat/temp
Using JRE_HOME:        /
Using CLASSPATH:        /root/tomcat/bin/bootstrap.jar:/root/tomcat/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
[root@ip-191-50-0-194 bin]# cd ..
[root@ip-191-50-0-194 tomcat]# cd webapps
[root@ip-191-50-0-194 webapps]# ls
docs  examples  host-manager  manager  ROOT
[root@ip-191-50-0-194 webapps]# sudo wget https://tomcat.apache.org/tomcat-6.0-doc/appdev/sample/sample.war
--2025-06-10 13:53:04--  https://tomcat.apache.org/tomcat-6.0-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... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4606 (4.5K)
Saving to: 'sample.war'

100%[=====] 4,606 --.-K/s in 0.00s

2025-06-10 13:53:04 (7.76 MB/s) - 'sample.war' saved [4606/4606]

[root@ip-191-50-0-194 webapps]# ls
docs  examples  host-manager  manager  ROOT  sample.war
[root@ip-191-50-0-194 webapps]# ll
total 12
drwxr-xr-x 16 root root 4096 Jun 10 13:51 docs
drwxr-xr-x  7 root root  99 Jun 10 13:51 examples
drwxr-xr-x  6 root root  79 Jun 10 13:51 host-manager
drwxr-xr-x  6 root root 114 Jun 10 13:51 manager
drwxr-xr-x  3 root root 223 Jun 10 13:51 ROOT
-rw-r--r--  1 root root 4606 Nov 16 2016 sample.war
[root@ip-191-50-0-194 webapps]# ll
total 12
drwxr-xr-x 16 root root 4096 Jun 10 13:51 docs
drwxr-xr-x  7 root root  99 Jun 10 13:51 examples
drwxr-xr-x  6 root root  79 Jun 10 13:51 host-manager
drwxr-xr-x  6 root root 114 Jun 10 13:51 manager
drwxr-xr-x  3 root root 223 Jun 10 13:51 ROOT
drwxr-xr-x  5 root root  86 Jun 10 13:53 sample
-rw-r--r--  1 root root 4606 Nov 16 2016 sample.war
[root@ip-191-50-0-194 webapps]#
```

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

```
aws ec2 run-instances 866018956544_vpcflowlogs_us-eas
File Edit View
|version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status
2 866018956544 eni-0a293212e9af42560 13.214.173.166 191.50.0.10 0 0 1 1 28 1749563987 1749563988 ACCEPT OK
```

CloudWatch

Log groups

my-first-log

eni-0bcbb8fc802908bfc-all

Log events

Filter events - press enter to search

1m1h

UTC timezone

Display

Timestamp	Message
2025-06-10T14:18:23.000Z	2 866018956544 eni-0bcbb8fc802908bfc 204.76.203.208 191.50.0.194 37259 444 6 1 40 1749565103 1749565124 A...
2025-06-10T14:18:23.000Z	2 866018956544 eni-0bcbb8fc802908bfc 191.50.0.194 204.76.203.208 444 37259 6 1 40 1749565103 1749565124 A...
2025-06-10T14:18:23.000Z	2 866018956544 eni-0bcbb8fc802908bfc 151.26.18.165 191.50.0.194 46279 23 6 1 44 1749565103 1749565124 ACC...
2025-06-10T14:18:23.000Z	2 866018956544 eni-0bcbb8fc802908bfc 191.50.0.194 151.26.18.165 23 46279 6 1 40 1749565103 1749565124 ACC...
2025-06-10T14:18:23.000Z	2 866018956544 eni-0bcbb8fc802908bfc 66.118.230.14 191.50.0.194 123 35240 17 1 76 1749565103 1749565124 A...
2025-06-10T14:18:23.000Z	2 866018956544 eni-0bcbb8fc802908bfc 191.50.0.194 66.118.230.14 35240 123 17 1 76 1749565103 1749565124 A...
2025-06-10T14:18:23.000Z	2 866018956544 eni-0bcbb8fc802908bfc 185.91.127.81 191.50.0.194 443 21414 6 1 52 1749565103 1749565124 AC...
2025-06-10T14:18:23.000Z	2 866018956544 eni-0bcbb8fc802908bfc 191.50.0.194 185.91.127.81 21414 443 6 1 40 1749565103 1749565124 AC...

Back to top

VPC

Your VPCs

Successfully created flow log for vpc-03f8a2ff2fc5f8333.

Your VPCs (1/2)

Find VPCs by attribute or tag

Name	VPC ID	State	Block Public...	IPv4 CIDR
mvvnr	vpc-03f8a2ff2fc5f8333	Available	Off	191.50.0.0/16

Details

Resource map

CIDRs

Flow logs

Tags

Integrations

Flow logs (2)

Search

Name	Flow log ID	Filter	Destination type	Destina
my_flowlog-s3	fl-0c21ba59208f1824d	ALL	s3	my-buc
my-first-cloudwatch	fl-0c986cae60775cfdd	ALL	cloud-watch-logs	my-first