

## AWS VPC Assignment Practical

### Step-1: Create SSH Key pair and download the .pem file.

#### Key pairs (1) [Info](#)

Find Key Pair by attribute or tag

<input type="checkbox"/>	Name	Type	Created
<input type="checkbox"/>	dipak-main-ssh	rsa	2025/07/09 19:49 GMT+5:30

### Step-2: Create a VPC

#### vpc-0b9e9ec9f299ec223 / MyVPC-vpc

##### Details [Info](#)

###### VPC ID

 vpc-0b9e9ec9f299ec223

###### DNS resolution

Enabled

###### Main network ACL

[acl-09022c1ba0674ad64](#)

###### IPv6 CIDR (Network border group)

–

###### State

 Available

###### Tenancy

default

###### Default VPC

No

###### Network Address Usage metrics

Disabled

###### Block Public Access

 Off

###### DHCP option set

[dopt-06070aeda2d199b8c](#)

###### IPv4 CIDR

10.0.0.0/16

###### Route 53 Resolver DNS Firewall rule groups

–

###### DNS hostnames

Enabled

###### Main route table

[rtb-0d11dd7b81a1352cf](#)

###### IPv6 pool

–

###### Owner ID

 076526621834

### Step-3: Create Public & Private Subnets

#### Subnets (4) [Info](#)

Last updated  
1 minute ago



Actions

Create subnet

Find subnets by attribute or tag

VPC: [vpc-0598323dd9c6f4f92](#)

Clear filters

< 1 >

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
<input type="checkbox"/>	Private-Subnet-1	<a href="#">subnet-045121416216b724e</a>	Available	<a href="#">vpc-0598323dd9c6f4f92</a>   <a href="#">My-V...</a>	Off	10.0.3.0/24
<input type="checkbox"/>	Private-Subnet-2	<a href="#">subnet-0a833b40f66846530</a>	Available	<a href="#">vpc-0598323dd9c6f4f92</a>   <a href="#">My-V...</a>	Off	10.0.4.0/24
<input type="checkbox"/>	Public-Subnet-2	<a href="#">subnet-0e44b3ccb7c06e33c</a>	Available	<a href="#">vpc-0598323dd9c6f4f92</a>   <a href="#">My-V...</a>	Off	10.0.2.0/24
<input type="checkbox"/>	Public-Subnet-1	<a href="#">subnet-08e2a5746d650353f</a>	Available	<a href="#">vpc-0598323dd9c6f4f92</a>   <a href="#">My-V...</a>	Off	10.0.1.0/24

### Step-4: Create Internet Gateway and attach it to VPC

#### igw-0f31f4f894ba5531d / MyVPC-IGW

##### Details [Info](#)

###### Internet gateway ID

 igw-0f31f4f894ba5531d

###### State

 Attached

###### VPC ID

[vpc-0598323dd9c6f4f92](#) | [My-VPC](#)

###### Owner

 076526

##### Tags

Search tags

Key	Value
Name	MyVPC-IGW

Step-5: Create NAT Gateway and ensure to allocate an elastic IP address

nat-051b2bda4b6a36698 / MyVPC-NAT

Details

<b>NAT gateway ID</b> nat-051b2bda4b6a36698	<b>Connectivity type</b> Public	<b>State</b> Available
<b>NAT gateway ARN</b> arn:aws:ec2:us-east-1:076526621834:natgateway/nat-051b2bda4b6a36698	<b>Primary public IPv4 address</b> 13.223.128.124	<b>Primary private IP</b> 10.0.1.13
<b>VPC</b> vpc-0598323dd9c6f4f92 / My-VPC	<b>Subnet</b> subnet-08e2a5746d650353f / Public-Subnet-1	<b>Created</b> Saturday, 12/12/2020 10:00:00 GMT+5:30

Step-6: Create Public & Private Route Tables and add routes

rtb-002f202af99e5de90 / Public-RT

Details

<b>Route table ID</b> rtb-002f202af99e5de90	<b>Main</b> No	<b>Explicit subnet associations</b> 2 subnets
<b>VPC</b> vpc-0598323dd9c6f4f92 / My-VPC	<b>Owner ID</b> 076526621834	<div>subnet-08e2a5746d650353f / Public-Subnet-1</div> <div>subnet-0e44b3ccb7c06e33c / Public-Subnet-2</div>

- Routes
- Subnet associations
- Edge associations
- Route propagation
- Tags

Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0f31f4f894ba5531d	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route

rtb-0f99d8d707b2be030 / Private-RT

Details

<b>Route table ID</b> rtb-0f99d8d707b2be030	<b>Main</b> No	<b>Explicit subnet associations</b> 2 subnets
<b>VPC</b> vpc-0598323dd9c6f4f92 / My-VPC	<b>Owner ID</b> 076526621834	<div>subnet-045121416216b724e / Private-Subnet-1</div> <div>subnet-0a833b40f66846530 / Private-Subnet-2</div>

- Routes
- Subnet associations
- Edge associations
- Route propagation
- Tags

Routes (2)


Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	nat-051b2bda4b6a36698	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route

Step-7: Associate Subnets with Route Tables

rtb-002f202af99e5de90 / Public-RT

Details [Info](#)


Route table ID

 rtb-002f202af99e5de90


VPC

[vpc-0598323dd9c6f4f92](#) | My-VPC

Main

 No

Owner ID


 076526621834

Explicit subnet associations

[2 subnets](#)

- Routes
- [Subnet associations](#)
- Edge associations
- Route propagation
- Tags

Explicit subnet associations (2)


 Find subnet association

Name	Subnet ID	IPv4 CIDR
Public-Subnet-2	<a href="#">subnet-0e44b3ccb7c06e33c</a>	10.0.2.0/24
Public-Subnet-1	<a href="#">subnet-08e2a5746d650353f</a>	10.0.1.0/24

rtb-0f99d8d707b2be030 / Private-RT

Details [Info](#)


Route table ID

 rtb-0f99d8d707b2be030


VPC

[vpc-0598323dd9c6f4f92](#) | My-VPC

Main

 No

Owner ID


 076526621834

Explicit subnet associations

[2 subnets](#)

- Routes
- [Subnet associations](#)
- Edge associations
- Route propagation
- Tags





Explicit subnet associations (2)


 Find subnet association

Name	Subnet ID	IPv4 CIDR
Private-Subnet-1	<a href="#">subnet-045121416216b724e</a>	10.0.3.0/24
Private-Subnet-2	<a href="#">subnet-0a833b40f66846530</a>	10.0.4.0/24

## Step-8: Create Security Groups



## sg-046fb9ed0ab9d9b34 - Bastion-SG

Details				
Security group name		Security group ID		Description
 Bastion-SG		 sg-046fb9ed0ab9d9b34		 SSH access for bastion host
Owner		Inbound rules count		Outbound rules count
 076526621834		1 Permission entry		1 Permission entry

Inbound rules (1)						<a href="#">Manage tags</a> <a href="#">Edit inbound rules</a>	
<input type="text" value="Search"/>						< 1 > 	
Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	
-	sgr-00ad1d889f95a6965	IPv4	SSH	TCP	22	223.184	

**sg-09472cbc2fc510f19 - Private-SG**

Details				
<b>Security group name</b> Private-SG		<b>Security group ID</b> sg-09472cbc2fc510f19		<b>Description</b> Access for private instances
<b>Owner</b> 076526621834		<b>Inbound rules count</b> 2 Permission entries		<b>VPC ID</b> <a href="#">vpc-0598323dd9c6f4f92</a>
		<b>Outbound rules count</b> 1 Permission entry		

Inbound rules (2)								Manage tags	Edit inbound rules	< 1 >	
Search											
Security group rule ID	IP version	Type	Protocol	Port range	Source	Description					
sg-09cd574a520084603	IPv4	All ICMP - IPv4	ICMP	All	10.0.0.0/16	-					
sg-040c971ee1d9686f3	-	SSH	TCP	22	<a href="#">sg-046fb9ed0ab9d9b3...</a>	-					

## Step-9: Launch EC2 Instances

Instances (2) [Info](#)

Connect

Instance state ▾

Actions ▾

Launch instances ▾

All states ▾

Instance state = running ✕

Clear filters

<

1

>

⚙️

<input type="checkbox"/>	Name  ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾	Public IP v.
<input type="checkbox"/>	Bastion Host	i-0c99fe5b6ab29d2c0	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<a href="#">View alarms +</a>	us-east-1a	-
<input type="checkbox"/>	Private-Instance	i-0f1d56230340c259a	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<a href="#">View alarms +</a>	us-east-1a	-

## Step-10: Connect to Instance

### Step-10.1: Copy the SSH key-pair from your local host to Bastion EC2 instance

```
[dipakprasad@Dipaks-MacBook-Pro Downloads % scp -i "dipak-main-ssh.pem" dipak-main-ssh.pem ec2-user@3.219.41.70:/home/ec2-user/dipak-main-ssh.pem  
dipak-main-ssh.pem                               100% 1678      4.3KB/s   00:00  
[dipakprasad@Dipaks-MacBook-Pro Downloads % ssh -i "dipak-main-ssh.pem" ec2-user@3.219.41.70  
  
#  
~\##### Amazon Linux 2023  
~\#####\  
~\#####\  
~\###|  
~\##/  
V~'---> https://aws.amazon.com/linux/amazon-linux-2023  
~'--  
~'--  
~'--  
~/m/'
```

Last login: Sat Oct 4 06:05:15 2025 from 223.184.140.40  
[ec2-user@ip-10-0-1-166 ~]\$ ls  
[dipak-main-ssh.pem]  
[ec2-user@ip-10-0-1-166 ~]\$ chmod 400 dipak-main-ssh.pem

## Step:10.2: Connect to Private Instance from Bastion host

```
[ec2-user@ip-10-0-1-166 ~]$ ls
[dipak-main-ssh.pem
[ec2-user@ip-10-0-1-166 ~]$ chmod 400 dipak-main-ssh.pem
[ec2-user@ip-10-0-1-166 ~]$ ssh -i dipak-main-ssh.pem ec2-user@10.0.3.132
The authenticity of host '10.0.3.132 (10.0.3.132)' can't be established.
ED25519 key fingerprint is SHA256:02ojQV9Px9W5t9aIog2YWXuedPJ9jK+401x+8fNpIdo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.132' (ED25519) to the list of known hosts.
```

[illegible]

## Step-11: Test your VPC setup

```
[ec2-user@ip-10-0-1-166 ~]$ ping google.com
PING google.com (142.251.179.113) 56(84) bytes of data:
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=1 ttl=109 time=1.72 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=2 ttl=109 time=1.71 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=3 ttl=109 time=1.71 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=4 ttl=109 time=1.72 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=5 ttl=109 time=1.69 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=6 ttl=109 time=1.72 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=7 ttl=109 time=1.73 ms
```

```
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 1.689/1.713/1.728/0.012 ms
```

```
[ec2-user@ip-10-0-1-166 ~]$ ls
dipak-main-ssh.pem
[ec2-user@ip-10-0-1-166 ~]$ ssh -i dipak-main-ssh.pem ec2-user@10.0.3.132
```

```

#_
~\_ ##### Amazon Linux 2023
~~ \#####\
~~ \|###|
~~ \|#/ https://aws.amazon.com/linux/amazon-linux-2023
~~ V~'-'>
~~~
~~~-.-
~/m/'

```

Last login: Sat Oct 4 06:08:14 2025 from 10.0.1.166

```
[ec2-user@ip-10-0-3-132 ~]$ ping google.com
PING google.com (142.251.179.101) 56(84) bytes of data:
64 bytes from pd-in-f101.1e100.net (142.251.179.101): icmp_seq=1 ttl=104 time=3.36 ms
64 bytes from pd-in-f101.1e100.net (142.251.179.101): icmp_seq=2 ttl=104 time=2.86 ms
64 bytes from pd-in-f101.1e100.net (142.251.179.101): icmp_seq=3 ttl=104 time=2.80 ms
64 bytes from pd-in-f101.1e100.net (142.251.179.101): icmp_seq=4 ttl=104 time=2.81 ms
64 bytes from pd-in-f101.1e100.net (142.251.179.101): icmp_seq=5 ttl=104 time=2.81 ms
```