

### Task 3. Build a VPC with Public & Private Subnets

Goal: Deploy infrastructure using networking best practices. Tasks:

- Create a VPC with 2 public and 2 private subnets.
- Configure route tables and Internet Gateway for public subnets.
- Set up a NAT Gateway for private subnets.
- Launch a public Bastion Host (EC2).
- Launch a private EC2 instance and connect to it through the Bastion using SSH.



#### 1. Create vpc

```
PS C:\Users\112256\k8\task\task-3\vpc-privatepublic-sub> aws ec2 describe-vpcs --filters Name=tag:Name,Values=devops-vpc
{
    "Vpcs": [
        {
            "OwnerId": "442955307475",
            "InstanceTenancy": "default",
            "CidrBlockAssociationSet": [
                {
                    "AssociationId": "vpc-cidr-assoc-00643a86f82737128",
                    "CidrBlock": "10.0.0.0/16",
                    "CidrBlockState": {
                        "State": "associated"
                    }
                }
            ],
            "IsDefault": false,
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "devops-vpc"
                }
            ],
            "BlockPublicAccessStates": {
                "InternetGatewayBlockMode": "off"
            },
            "VpcId": "vpc-0aa3d424782e7688c",
            "State": "available",
            "CidrBlock": "10.0.0.0/16".
        }
    ]
}
```

Your VPCs (1/1) [Info](#)

Name	VPC ID	State	Encryption c...	Encryption contr...
<a href="#">devops-vpc</a>	vpc-0aa3d424782e7688c	Available	-	-

**vpc-0aa3d424782e7688c / devops-vpc**

VPC ID <a href="#">vpc-0aa3d424782e7688c</a>	State <span style="color: green;">Available</span>	BLOCK PUBLIC ACCESS Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-0ef344d0193a5e7f8	Main route table rtb-02262de5cbda85fb2
Main network ACL acl-0a9ada6189605dbce	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -

## 2. Create public and private subnet

- Public subnets → internet-facing resources
- Private subnets → internal workloads

```
PS C:\Users\112256\k8\task\task-3\vpc-privatepublic-sub> aws ec2 describe-subnets --filters Name=vpc-id,Values=vpc-0aa3d424782e7688c
{
    "Subnets": [
        {
            "AvailabilityZoneId": "use1-az2",
            "MapCustomerOwnedIpOnLaunch": false,
            "OwnerId": "442955307475",
            "AssignIpv6AddressOnCreation": false,
            "Ipv6CidrBlockAssociationSet": [],
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "private-subnet-2"
                }
            ],
            "SubnetArn": "arn:aws:ec2:us-east-1:442955307475:subnet/subnet-0d283e94c59743bec",
            "EnableDns64": false,
            "Ipv6Native": false,
            "PrivateDnsNameOptionsOnLaunch": {
                "HostnameType": "ip-name",
                "EnableResourceNameDnsARecord": false,
                "EnableResourceNameDnsAAAARecord": false
            },
            "BlockPublicAccessStates": {
                "InternetGatewayBlockMode": "off"
            }
        }
    ]
}
```

```
        },
        "SubnetId": "subnet-0d283e94c59743bec",
        "State": "available",
        "VpcId": "vpc-0aa3d424782e7688c",
        "CidrBlock": "10.0.12.0/24",
        "AvailableIpAddressCount": 251,
        "AvailabilityZone": "us-east-1b",
        "DefaultForAz": false,
        "MapPublicIpOnLaunch": false
    },
    {
        "AvailabilityZoneId": "use1-az1",
        "MapCustomerOwnedIpOnLaunch": false,
        "OwnerId": "442955307475",
        "AssignIpv6AddressOnCreation": false,
        "Ipv6CidrBlockAssociationSet": [],
        "Tags": [
            {
                "Key": "Name",
                "Value": "private-subnet-1"
            }
        ],
        "SubnetArn": "arn:aws:ec2:us-east-1:442955307475:subnet/subnet-0aac7ea9bddb93858",
        "EnableDns64": false,
        "Ipv6Native": false,
        "PrivateDnsNameOptionsOnLaunch": {
            "HostnameType": "ip-name",
            "MapCustomerOwnedIpOnLaunch": false,
            "OwnerId": "442955307475",
            "AssignIpv6AddressOnCreation": false,
            "Ipv6CidrBlockAssociationSet": [],
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "public-subnet-2"
                }
            ],
            "SubnetArn": "arn:aws:ec2:us-east-1:442955307475:subnet/subnet-0849d38f7e7bd1616",
            "EnableDns64": false,
            "Ipv6Native": false,
            "PrivateDnsNameOptionsOnLaunch": {
                "HostnameType": "ip-name",
                "EnableResourceNameDnsARecord": false,
                "EnableResourceNameDnsAAAARecord": false
            },
            "BlockPublicAccessStates": {
                "InternetGatewayBlockMode": "off"
            },
            "SubnetId": "subnet-0849d38f7e7bd1616",
            "State": "available",
            "VpcId": "vpc-0aa3d424782e7688c",
            "CidrBlock": "10.0.2.0/24",
            "AvailableIpAddressCount": 251,
            "AvailabilityZone": "us-east-1b",
            "MapCustomerOwnedIpOnLaunch": false
        }
    }
]
```

**Subnets (4/4) Info**

Last updated less than a minute ago

**Actions** | **Create subnet**

Name	Subnet ID	State	VPC
private-subnet-2	subnet-0d283e94c59743bec	Available	vpc-0aa3d424782e7688c   dev...
private-subnet-1	subnet-0aac7ea9bddb93858	Available	vpc-0aa3d424782e7688c   dev...
public-subnet-2	subnet-0849d38f7e7bd1616	Available	vpc-0aa3d424782e7688c   dev...
public-subnet-1	subnet-08436d22decb6cb8c	Available	vpc-0aa3d424782e7688c   dev...

**Subnets:** subnet-0d283e94c59743bec, subnet-0aac7ea9bddb93858, subnet-0849d38f7e7bd1616, subnet-08436d22decb6cb8c

### 3. Configure route tables and Internet Gateway for public subnets.

```
$S C:\Users\112256\k8\task\task-3\vpc-privatepublic-sub> aws ec2 describe-route-tables --filters Name=tag:Name,Values=public-rt
{
    "RouteTables": [
        {
            "Associations": [
                {
                    "Main": false,
                    "RouteTableAssociationId": "rtbassoc-00a97f2b60afe9a0a",
                    "RouteTableId": "rtb-0e50f75ee3db8f667",
                    "SubnetId": "subnet-0849d38f7e7bd1616",
                    "AssociationState": {
                        "State": "associated"
                    }
                },
                {
                    "Main": false,
                    "RouteTableAssociationId": "rtbassoc-0f3a2c4089de37fef",
                    "RouteTableId": "rtb-0e50f75ee3db8f667",
                    "SubnetId": "subnet-08436d22decb6cb8c",
                    "AssociationState": {
                        "State": "associated"
                    }
                }
            ]
        }
    ]
}
```

```

        ],
        "PropagatingVgws": [],
        "RouteTableId": "rtb-0e50f75ee3db8f667",
        "Routes": [
            {
                "DestinationCidrBlock": "10.0.0.0/16",
                "GatewayId": "local",
                "Origin": "CreateRouteTable",
                "State": "active"
            },
            {
                "DestinationCidrBlock": "0.0.0.0/0",
                "GatewayId": "igw-002a3dff403fb3a5",
                "Origin": "CreateRoute",
                "State": "active"
            }
        ],
        "Tags": [
            {
                "Key": "Name",
                "Value": "public-rt"
            }
        ]
    ],

```

**VPC > Route tables**

**Route tables (1/2) Info**

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main
<input checked="" type="checkbox"/> public-rt	rtb-0e50f75ee3db8f667	2 subnets	-	No
<input type="checkbox"/> -	rtb-02262de5cbda85fb2	-	-	Yes

**rtb-0e50f75ee3db8f667 / public-rt**

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-002a3dff403fb3a5	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

**VPC > Internet gateways**

**Internet gateways (1) Info**

Name	Internet gateway ID	State	VPC ID
<input type="checkbox"/> devops-igw	igw-002a3dff403fb3a5	Attached	vpc-0aa3d424782e7688c   devc

Select an internet gateway above

#### 4. Set up a NAT Gateway for private subnets.

**Use - Private instances need outbound internet access securely.**

```
PS C:\Users\112256\k8\task\task-3\vpc-privatepublic-sub> aws ec2 describe-nat-gateways
{
    "NatGateways": [
        {
            "CreateTime": "2025-12-17T06:56:03+00:00",
            "NatGatewayAddresses": [
                {
                    "AllocationId": "eipalloc-066f396ae87b4587c",
                    "NetworkInterfaceId": "eni-084f54e78837df00e",
                    "PrivateIp": "10.0.1.71",
                    "PublicIp": "44.212.134.19",
                    "AssociationId": "eipassoc-017930b80b955982e",
                    "IsPrimary": true,
                    "Status": "succeeded"
                }
            ],
            "NatGatewayId": "nat-071d1d35d1c665ce1",
            "State": "available",
            "SubnetId": "subnet-08436d22decb6cb8c",
            "VpcId": "vpc-0aa3d424782e7688c",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "nat-gateway"
                }
            ],
            "ConnectivityType": "public"
        }
    ]
}
```

Name	NAT gateway ID	Connectivity...	State	State message	Available
nat-gateway	nat-071d1d35d1c665ce1	Public	Available	-	Zonal

  

nat-071d1d35d1c665ce1 / nat-gateway					
NAT gateway ID	Connectivity type	State		State message	
nat-071d1d35d1c665ce1	Public	Available		-	
NAT gateway ARN	Primary public IPv4 address	Primary private IPv4 address		Primary network interface ID	
arn:aws:ec2:us-east-1:442955307475:natgateway/nat-071d1d35d1c665ce1	44.212.134.19	10.0.1.71		eni-084f54e78837df00e	
Subnet	Created	Deleted			

## 5.Launch a public Bastion Host (EC2).

- Use for - Single secure SSH entry point.

```
connection to 44.192.109.99 closed.
PS C:\Users\112256\k8\task\task-3\vpc-privatepublic-sub> aws ec2 describe-instances --filters Name=tag:Name,Values=bastion
-host --query "Reservations[].[Instances[].PublicIpAddress" --output text
44.192.109.99
)
PS C:\Users\112256\k8\task\task-3\vpc-privatepublic-sub> ssh -i my-key.pem ec2-user@44.192.109.99
Last login: Wed Dec 17 07:45:07 2025 from 182.19.89.145
      #
~\_ ##### Amazon Linux 2
~~ \#####\ AL2 End of Life is 2025-06-30.
~~  \###| \#/ ___
~~   \~' '-'>
~~    / 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/

51 package(s) needed for security, out of 69 available
Run "sudo yum update" to apply all updates.
Last login: Wed Dec 17 07:45:07 2025 from 182.19.89.145
      #
~\_ ##### Amazon Linux 2
~~ \#####\ AL2 End of Life is 2025-06-30.

,
~\_ ##### Amazon Linux 2
~~ \#####\ AL2 End of Life is 2025-06-30.
~~  \###| \#/ ___
~~   \~' '-'>
~~    / 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/

51 package(s) needed for security, out of 69 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-173 ~]$ ls
[ec2-user@ip-10-0-1-173 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-1-173 ~]$ []
```

The screenshot shows the AWS EC2 Instances summary page for a specific instance. The instance ID is i-0ace74f8fec0a3dd3, and its state is Running. It has a Public IPv4 address of 44.192.109.99 and a Private IP DNS name (IPv4 only) of ip-10-0-1-173.ec2.internal. The instance type is t2.micro, and it is associated with VPC ID vpc-0aa3d424782e7688c. The public DNS is ec2-44-192-109-99.compute-1.amazonaws.com. There is also a note about AWS Compute Optimizer finding.

**Instance summary for i-0ace74f8fec0a3dd3 (bastion-host)**

**Connect** **Instance state** **Actions**

Updated less than a minute ago

Attribute	Value
Instance ID	i-0ace74f8fec0a3dd3
IPv6 address	-
Hostname type	IP name: ip-10-0-1-173.ec2.internal
Answer private resource DNS name	-
Auto-assigned IP address	44.192.109.99 [Public IP]
Public IPv4 address	44.192.109.99   open address
Instance state	Running
Private IP DNS name (IPv4 only)	ip-10-0-1-173.ec2.internal
Instance type	t2.micro
VPC ID	vpc-0aa3d424782e7688c (devops-vpc)
Private IPv4 addresses	10.0.1.173
Public DNS	ec2-44-192-109-99.compute-1.amazonaws.com   open address
Elastic IP addresses	-
AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations.

6. Launch a private EC2 instance and connect to it through the Bastion using SSH.

The screenshot shows the AWS EC2 Instances summary page for a private instance. The instance ID is i-0654b9b5c4a8c0f92, and its state is Running. It has a Public IP DNS name (IPv4 only) of ip-10-0-11-122.ec2.internal and a Private IP DNS name (IPv4 only) of ip-10-0-11-122.ec2.internal. The instance type is t2.micro, and it is associated with VPC ID vpc-0aa3d424782e7688c. The public DNS is ec2-10-0-11-122.compute-1.amazonaws.com. There is also a note about AWS Compute Optimizer finding.

**Instance summary for i-0654b9b5c4a8c0f92 (private-instance)**

**Connect** **Instance state** **Actions**

Updated less than a minute ago

Attribute	Value
Instance ID	i-0654b9b5c4a8c0f92
IPv6 address	-
Hostname type	IP name: ip-10-0-11-122.ec2.internal
Answer private resource DNS name	-
Auto-assigned IP address	-
Public IPv4 address	-
Instance state	Running
Private IP DNS name (IPv4 only)	ip-10-0-11-122.ec2.internal
Instance type	t2.micro
VPC ID	vpc-0aa3d424782e7688c (devops-vpc)
Private IPv4 addresses	10.0.11.122
Public DNS	-
Elastic IP addresses	-
AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations.

```
> PS C:\Users\112256\k8\task\task-3\vpc-privatepublic-sub> ssh -i .\my-key.pem ec2-user@44.192.109.99
Last login: Wed Dec 17 07:50:01 2025 from 182.19.89.145
      #_
~\_ #####_          Amazon Linux 2
~~ \#####\
~~ \###|          AL2 End of Life is 2025-06-30.
~~ \#/ ---_
~~ 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/

51 package(s) needed for security, out of 69 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-173 ~]$ ls
[ec2-user@ip-10-0-1-173 ~]$ ssh ec2-user@10.0.11.122
The authenticity of host '10.0.11.122 (10.0.11.122)' can't be established.
ECDSA key fingerprint is SHA256:m5dquWQnaXfwLJdJUFD/gNoX90t2ctHbDycatQ44ktY.
ECDSA key fingerprint is MD5:c1:e3:93:2a:df:f8:ed:05:61:d6:ee:17:85:bc:50:9d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.11.122' (ECDSA) to the list of known hosts.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-1-173 ~]$ █
```

```
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-1-173 ~]$ ping google.com
PING google.com (142.251.163.101) 56(84) bytes of data.
64 bytes from wv-in-f101.1e100.net (142.251.163.101): icmp_seq=1 ttl=102 time=2.04 ms
64 bytes from wv-in-f101.1e100.net (142.251.163.101): icmp_seq=2 ttl=102 time=2.05 ms
64 bytes from wv-in-f101.1e100.net (142.251.163.101): icmp_seq=3 ttl=102 time=2.01 ms
64 bytes from wv-in-f101.1e100.net (142.251.163.101): icmp_seq=4 ttl=102 time=2.05 ms
64 bytes from wv-in-f101.1e100.net (142.251.163.101): icmp_seq=5 ttl=102 time=2.04 ms
64 bytes from wv-in-f101.1e100.net (142.251.163.101): icmp_seq=6 ttl=102 time=2.03 ms
64 bytes from wv-in-f101.1e100.net (142.251.163.101): icmp_seq=7 ttl=102 time=2.03 ms
64 bytes from wv-in-f101.1e100.net (142.251.163.101): icmp_seq=8 ttl=102 time=2.08 ms
█
```