



AWS VPC Assignment

Step 1: Create SSH Key Pair

 Successfully created key pair

Key pairs (1) [Info](#)

 Find Key Pair by attribute or tag

| <input type="checkbox"/> | Name | Type |
|--------------------------|------------|------|
| <input type="checkbox"/> | my-vpc-key | rsa |

Step 2: Create VPC

vpc-07d2d7f97534b834e / MyVPC

Details

Info

VPC ID

vpc-07d2d7f97534b834e

DNS resolution

Enabled

Main network ACL

acl-017f4c1b062530e59

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-061b428419b097b52

IPv4 CIDR

10.0.0.0/16

Route 53 Resolver DNS Firewall rule groups

–

Step 3: Create Internet Gateway

igw-09d267a106708f221 / MyVPC-IGW

Details

Info

Internet gateway ID

igw-09d267a106708f221

State

Attached

VPC ID

vpc-07d2d7f97534b834e | MyVPC

Tags

Search tags

Key

Value

Name

MyVPC-IGW

Step 4: Create Subnets

| Name | Subnet ID | State | IPv4 CIDR |
|------------------|--------------------------|-----------|-------------|
| Public-Subnet-1 | subnet-0ffc0d70540d9d5d9 | Available | 10.0.1.0/24 |
| Public-Subnet-2 | subnet-07cd8b20761170488 | Available | 10.0.2.0/24 |
| Private-Subnet-1 | subnet-008b9a552d348cdd3 | Available | 10.0.3.0/24 |
| Private-Subnet-2 | subnet-07b43612c78200147 | Available | 10.0.4.0/24 |

Step 5: Create NAT Gateway

nat-0427fa6c35746a15c / MyVPC-NAT

Details

NAT gateway ID

nat-0427fa6c35746a15c

NAT gateway ARN

arn:aws:ec2:us-east-1:307946636515:natgateway/nat-0427fa6c35746a15c

VPC

vpc-07d2d7f97534b834e / MyVPC

Connectivity type

Public

Primary public IPv4 address

44.199.88.116

Subnet


subnet-0ffc0d70540d9d5d9 / Public-Subnet-1

Step 6: Create Route Tables

rtb-0026a73ca15ad7f8b / Public-RT

Details [Info](#)

Route table ID

 rtb-0026a73ca15ad7f8b

VPC

[vpc-07d2d7f97534b834e](#) | MyVPC

Main

 No

Owner ID

 307946636515

[Routes](#)

[Subnet associations](#)

[Edge associations](#)

[Route propagation](#)

[Tags](#)

Routes (2)



| Destination | Target | Status |
|-------------|---------------------------------------|----------|
| 0.0.0.0/0 | igw-09d267a106708f221 | ✓ Active |
| 10.0.0.0/16 | local | ✓ Active |

rtb-044c102a663241972 / Private-RT

Details [Info](#)

Route table ID

 rtb-044c102a663241972


VPC

[vpc-07d2d7f97534b834e](#) | MyVPC

Main

 No

Owner ID

 307946636515

[Routes](#)

[Subnet associations](#)

[Edge associations](#)

[Route propagation](#)

[Tags](#)

Routes (2)



| Destination | Target | Status |
|-------------|---------------------------------------|----------|
| 0.0.0.0/0 | nat-0427fa6c35746a15c | ✓ Active |
| 10.0.0.0/16 | local | ✓ Active |

sg-027ebeca9b3f94370 - Private-SG

Details

Security group name
Private-SG

Security group ID
sg-027ebeca9b3f94370

Description
Private-SG: Access for private instances

Owner
307946636515

Inbound rules count
2 Permission entries

Outbound rules count
1 Permission entry

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

Inbound rules (2)

| <input type="checkbox"/> | Name | Security group rule ID | IP version | Type | Protocol | Port |
|--------------------------|------|------------------------|------------|-----------------|----------|------|
| <input type="checkbox"/> | - | sgr-080438ed22a6f8d2e | IPv4 | All ICMP - IPv4 | ICMP | All |
| <input type="checkbox"/> | - | sgr-06348703ab02891ea | - | SSH | TCP | 22 |

Step 9: Launch EC2 Instances

Instances (2) Info

Find Instance by attribute or tag (case-sensitive)

| <input type="checkbox"/> | Name | Instance ID | Instance state | Instance type |
|--------------------------|------------------|---------------------|----------------|---------------|
| <input type="checkbox"/> | Bastion-Host | i-06e68037eb3b7caa1 | Running | t2.micro |
| <input type="checkbox"/> | Private-Instance | i-0bcc3fa827f539a2a | Running | t2.micro |

Step 10: Connect to Instances

```
Admin@DESKTOP-AFSF9SU MINGW64 /d/devops_codes
$ chmod 400 my-vpc-key.pem

Admin@DESKTOP-AFSF9SU MINGW64 /d/devops_codes
$ ls -l my-vpc-key.pem
-r--r--r-- 1 Admin 197121 1679 Sep 10 10:49 my-vpc-key.pem
```



```

ec2-user@private-instance ~]$ 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=105 time=3.04 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=2 ttl=105 time=2.42 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=3 ttl=105 time=2.39 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=4 ttl=105 time=2.42 ms
64 bytes from pd-in-f113.1e100.net (142.251.179.113): icmp_seq=5 ttl=105 time=2.44 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.387/2.542/3.041/0.249 ms
ec2-user@private-instance ~]$ exit
exit
connection to 10.0.3.23 closed.
ec2-user@bastion-host ~]$ ping google.com
PING google.com (172.253.63.138) 56(84) bytes of data.
64 bytes from bi-in-f138.1e100.net (172.253.63.138): icmp_seq=1 ttl=106 time=2.38 ms
64 bytes from bi-in-f138.1e100.net (172.253.63.138): icmp_seq=2 ttl=106 time=2.42 ms
64 bytes from bi-in-f138.1e100.net (172.253.63.138): icmp_seq=3 ttl=106 time=2.53 ms
64 bytes from bi-in-f138.1e100.net (172.253.63.138): icmp_seq=4 ttl=106 time=2.46 ms
64 bytes from bi-in-f138.1e100.net (172.253.63.138): icmp_seq=5 ttl=106 time=2.42 ms
^C

```

Step 10: Load Balancer Setup

Create Target Group

TG1

Details

 [arn:aws:elasticloadbalancing:us-east-1:307946636515:targetgroup/TG1/;](#)

Target type

Instance

Protocol : Port

HTTP: 80

IP address type

IPv4

Load balancer

[my-alb1](#) 

| TARGETS | Monitoring | Health checks | Attributes | Tags | | | | | | | | | | | | | | | |
|---|-------------------------------------|--------------------|------------|-------------------|--------------------------|-------------|------|------|------|--------------------------|-------------------------------------|--------------------|----|-------------------|--------------------------|-------------------------------------|------------------|----|-------------------|
| <h2>Registered targets (2) Info</h2> <p>Target groups route requests to individual registered targets using the protocol and port number specified. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.</p> <div> <input type="text"/> </div> <table> <tr> <th><input type="checkbox"/></th><th>Instance ID</th><th>Name</th><th>Port</th><th>Zone</th></tr> <tr> <td><input type="checkbox"/></td><td>i-0af2858452d45d1da</td><td>Private-Instanc...</td><td>80</td><td>us-east-1b (us...</td></tr> <tr> <td><input type="checkbox"/></td><td>i-0bcc3fa827f539a2a</td><td>Private-Instance</td><td>80</td><td>us-east-1a (us...</td></tr> </table> | | | | | <input type="checkbox"/> | Instance ID | Name | Port | Zone | <input type="checkbox"/> | i-0af2858452d45d1da | Private-Instanc... | 80 | us-east-1b (us... | <input type="checkbox"/> | i-0bcc3fa827f539a2a | Private-Instance | 80 | us-east-1a (us... |
| <input type="checkbox"/> | Instance ID | Name | Port | Zone | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | i-0af2858452d45d1da | Private-Instanc... | 80 | us-east-1b (us... | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | i-0bcc3fa827f539a2a | Private-Instance | 80 | us-east-1a (us... | | | | | | | | | | | | | | | |

Create ALB

my-alb1

▼ Details

Load balancer type

Application

Scheme

Internet-facing

Status

✔ Active

Hosted zone

Z355XDOTRQ7X7K

VPC

[vpc-07d2d7f97534b834e](#)

Availability Zones

[subnet-0ffc0d70540d9d5d9](#) us-east-1a (use1-az1)

[subnet-07cd8b20761170488](#) us-east-1b (use1-az2)

Load balancer ARN

[arn:aws:elasticloadbalancing:us-east-1:307946636515:loadbalancer/app/my-alb1/bf1c8f308e58cb7f](#)

DNS name

Info

[my-alb1-1090763256.us-east-1.elb.amazonaws.com](#)

Listeners and rules

Network mapping

Resource map

Security

Monitoring

Integrations

Attributes

Capacity

Listeners and rules (1)

Info

Manage rules

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional actions.

Q Filter listeners

☐

Protocol:Port

▼

Default action

▼

Rules

▼

ARN

▼

Security policy

☐

[HTTP:80](#)

• Forward to target group

[TG1](#) 1 (100%)

[1 rule](#)

[ARN](#)

Not applicable

Security groups — important

- ALB SG (sg-alb): inbound 80 (or 443) from 0.0.0.0/0. Outbound to anywhere (default).

- App EC2 SG (sg-app): DO NOT open port 80 to 0.0.0.0/0. Instead add an inbound rule allowing the ALB SG as the source:
- Type: Custom TCP (port 80)
- Source: sg-alb (use the ALB security group id)
- This ensures only ALB can talk to your private instances on the app port.
- Console path: EC2 → Security Groups → Select sg-app → Edit inbound rules → Add rule → choose “Custom” and enter the ALB SG id in “Source”.

Test the ALB

<http://my-alb1-1090763256.us-east-1.elb.amazonaws.com/>

private-instance-1

private-instance2