

VPC and Peering

It's a five tier Architecture

Problem Statement:

You work for XYZ Corporation and based on the expansion requirements of your corporation you have been asked to create and set up a distinct Amazon VPC for the production and development team. You are expected to perform the following tasks for the respective VPCs.

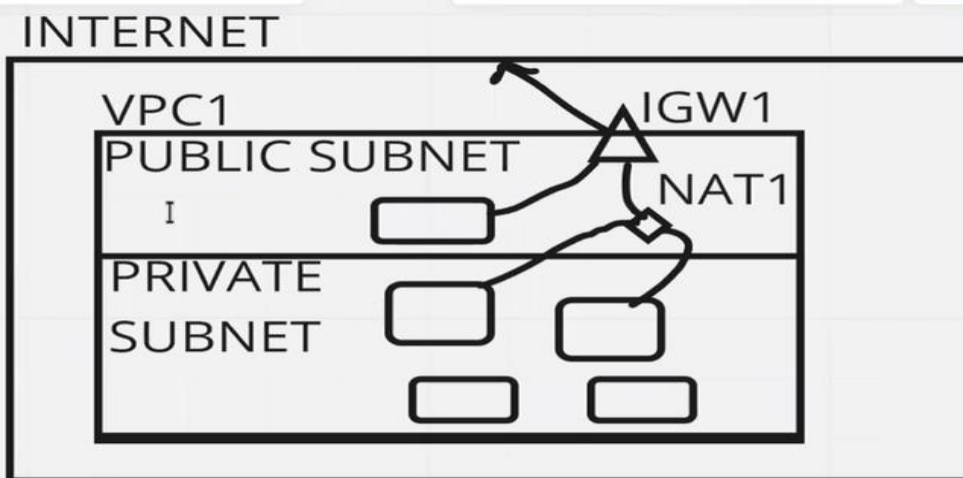
Production Network:

1. Design and build a 5-tier architecture.
2. Create 5 subnets out of which 4 should be private named app1, app2, dbcache and db and one should be public, named web.
3. Launch instances in all subnets and name them as per the subnet that they have been launched in.
4. Allow dbcache instance and app1 subnet to send internet requests.
5. Manage security groups and NACLs.

Development Network:

1. Design and build 2-tier architecture with two subnets named web and db and launch instances in both subnets and name them as per the subnet names.
2. Make sure only the web subnet can send internet requests.
3. Create peering connection between production network and development network.
4. Setup connection between db subnets of both production network and development network respectively.

Search for VPC service – go in vpc – choose create vpc.



[VPC](#) > [Your VPCs](#) > [Create VPC](#)

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

vpc-1

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

11.11.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

IPv4 CIDR

11.11.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name

Value - optional

Q vpc-1

Remove tag

Add tag

You can add 49 more tags

Cancel

Create VPC

While creating the vpc the one route table is self create and we have to create two more route table.

Route tables (4) Info

Find resources by attribute or tag

Actions

Create route table

< 1 >

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC
<input type="checkbox"/>	vpc-1-public	rtb-084c98d1a26986e99	–	–	Yes	vpc-021081f16040
<input type="checkbox"/>	–	rtb-08a8fe9c1597ac77e	–	–	Yes	vpc-080f6a5ebfa0d
<input type="checkbox"/>	vpc-1-private	rtb-024f1b7f09f139fa5	–	–	No	vpc-021081f16040
<input type="checkbox"/>	vpc-1-no-int	rtb-0d0c884a471cc2db3	–	–	No	vpc-021081f16040

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

vpc-1-private

VPC

The VPC to use for this route table.

vpc-021081f1604067f96 (vpc-1)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

Q Name

Q vpc-1-private

Remove

Add new tag

You can add 49 more tags.

Cancel

Create route table

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

vpc-1-no-int

VPC

The VPC to use for this route table.

vpc-021081f1604067f96 (vpc-1)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

Q Name

Q vpc-1-no-int

Remove

Add new tag

You can add 49 more tags.

Cancel

Create route table

Create four subnet public-1, private 1,2,3.

[VPC](#) > [Subnets](#) > Create subnet

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

vpc-021081f1604067f96 (vpc-1) ▼

Associated VPC CIDRs

IPv4 CIDRs

11.11.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 4

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

public-1

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Europe (Stockholm) / eu-north-1a ▼

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

11.11.0.0/16 ▼

IPv4 subnet CIDR block

11.11.1.0/24 256 IPs

< > ^ v

▼ Tags - optional

Key

Value - optional

Q Name X

Q public-1 X

Remove

Add new tag

You can add 49 more tags.

Remove

Subnet 2 of 4

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

private-1

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

11.11.0.0/16

IPv4 subnet CIDR block

11.11.2.0/24 256 IPs

< > ^ v

▼ Tags - optional

Key

Q Name X

Value - optional

Q private-1 X

Remove

Add new tag

You can add 49 more tags.

Remove

Subnet 4 of 4

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

private-3

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

11.11.0.0/16

IPv4 subnet CIDR block

11.11.4.0/24 256 IPs

< > ^ v

▼ Tags - optional

Key

Q Name X

Value - optional

Q private-3 X

Remove

Add new tag

You can add 49 more tags.

Remove

Subnet 3 of 4

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

private-2

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

11.11.0.0/16

IPv4 subnet CIDR block

11.11.3.0/24 256 IPs

< > ^ v

▼ Tags - optional

Key

Q Name X

Value - optional

Q private-2 X

Remove

Add new tag

You can add 49 more tags.

Remove

<input type="checkbox"/>	Name ▾	Subnet ID ▾	State ▾	VPC ▾	IPv4 CIDR
<input type="checkbox"/>	private-1	subnet-0d4294a4c225cb3bf	✔ Available	vpc-021081f1604067f96 vpc-1	11.11.2.0/24
<input type="checkbox"/>	private-2	subnet-0bb8367d00d8f2527	✔ Available	vpc-021081f1604067f96 vpc-1	11.11.3.0/24
<input type="checkbox"/>	private-3	subnet-0f52df4fa5788cddd	✔ Available	vpc-021081f1604067f96 vpc-1	11.11.4.0/24
<input type="checkbox"/>	public-1	subnet-0c6df3beb5f338064	✔ Available	vpc-021081f1604067f96 vpc-1	11.11.1.0/24

After creating the subnet we need to create internet gateway and attach to vpc.

[VPC](#) > [Internet gateways](#) > [Create internet gateway](#)

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

vpc-1-igw

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="vpc-1-igw"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

[VPC](#) > [Internet gateways](#) > [Attach to VPC \(igw-0f5dfc926a8bd82c8\)](#)

Attach to VPC (igw-0f5dfc926a8bd82c8) Info

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

☒ The following internet gateway was created: igw-0f5dfc926a8bd82c8 - vpc-1-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.

[VPC](#) > [Internet gateways](#) > [igw-0f5dfc926a8bd82c8](#)

igw-0f5dfc926a8bd82c8 / vpc-1-igw

▾

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0f5dfc926a8bd82c8	Detached	-	170303796048

Tags

Key	Value
Name	vpc-1-igw

After creating the IGW we need to create Nat gateway and allocate elastic IP.

✓ Elastic IP address 51.20.227.37 (eipalloc-0c2f9628053d2f953) allocated.

VPC > NAT gateways > Create NAT gateway

Create NAT gateway [Info](#)

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

vpc-1-nat

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

subnet-0c6df3beb5f338064 (public-1)

Connectivity type

Select a connectivity type for the NAT gateway.

☒ Public

☐ Private

Elastic IP allocation ID [Info](#)

Assign an Elastic IP address to the NAT gateway.

eipalloc-0c2f9628053d2f953

Allocate Elastic IP

▶ Additional settings [Info](#)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

🔍 Name

×

Value - *optional*

🔍 vpc-1-nat

×

Remove

Add new tag

You can add 49 more tags.

Cancel

Create NAT gateway

rtb-084c98d1a26986e99 / vpc-1-public

Actions ▾

Details [Info](#)

Route table ID 📄 rtb-084c98d1a26986e99	Main 📄 Yes	Explicit subnet associations -	Edge associations -
VPC vpc-021081f1604067f96 vpc-1	Owner ID 📄 170303796048		

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

Routes (1)

Both ▾

Edit routes

🔍 Filter routes

< 1 > ⚙️

Destination ▾	Target ▾	Status ▾	Propagated ▾
11.11.0.0/16	local	🟢 Active	No

Edit routes

Destination	Target	Status	Propagated
11.11.0.0/16	<div>local ▾</div> <div>🔍 local ✕</div>	🟢 Active	No
<div>🔍 0.0.0.0/0 ✕</div>	<div>Internet Gateway ▾</div> <div>🔍 igw- ✕</div>	-	No

Add route

Remove

Cancel

Preview

Save changes

Move in public route table – go on edit route – choose internet gateway – save changes.

Next associate subnet public one with same Route table.

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

Explicit subnet associations (1)

🔍 Find subnet association

Name ▾	Subnet ID ▾	IPv4 CIDR
public-1	subnet-0c6df3beb5f338064	11.11.1.0/24

Again do the same with Private-1 route table – edit route and associate subnet .

Edit routes

Destination	Target	Status	Propagated
11.11.0.0/16	<div>local</div> <div>Q local</div>	Active	No
<div>Q 0.0.0.0/0</div>	<div>NAT Gateway</div> <div>Q nat-0253953185406f5e6</div>	-	No

Remove

Add route

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Q Filter subnet associations

< 1 >

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	private-1	subnet-0d4294a4c225cb3bf	11.11.2.0/24	-	Main (rtb-084c98d1a26986e99 / vpc-1
<input checked="" type="checkbox"/>	private-2	subnet-0bb8367d00d8f2527	11.11.3.0/24	-	Main (rtb-084c98d1a26986e99 / vpc-1
<input type="checkbox"/>	private-3	subnet-0f52df4fa5788cddd	11.11.4.0/24	-	Main (rtb-084c98d1a26986e99 / vpc-1
<input type="checkbox"/>	public-1	subnet-0c6df3beb5f338064	11.11.1.0/24	-	rtb-084c98d1a26986e99 / vpc-1-publi

Selected subnets

subnet-0d4294a4c225cb3bf / private-1

subnet-0bb8367d00d8f2527 / private-2

As with no internet route table we don't need to edit route because it doesn't have internet connectivity, only associate subnet .

VPC > Route tables > rtb-0d0c884a471cc2db3 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/4)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	private-1	subnet-0d4294a4c225cb3bf	11.11.2.0/24	-	rtb-024f1b7f09f139fa5 / vpc-1-private
<input type="checkbox"/>	private-2	subnet-0bb8367d00d8f2527	11.11.3.0/24	-	rtb-024f1b7f09f139fa5 / vpc-1-private
<input checked="" type="checkbox"/>	private-3	subnet-0f52df4fa5788cddd	11.11.4.0/24	-	Main (rtb-084c98d1a26986e99 / vpc-1
<input type="checkbox"/>	public-1	subnet-0c6df3beb5f338064	11.11.1.0/24	-	rtb-084c98d1a26986e99 / vpc-1-publi

Selected subnets

subnet-0f52df4fa5788cddd / private-3

Cancel Save associations

Now we are going to launch instances in each public subnets using vpc-1.

Launch instance one in public subnet , vpc-1 with elastic ip enable and security group with all traffic allowed .

Network settings

VPC - required

vpc-021081f1604067f96 (vpc-1)
11.11.0.0/16

Subnet

subnet-0c6df3beb5f338064
VPC: vpc-021081f1604067f96 Owner: 170303796048
Availability Zone: eu-north-1a IP addresses available: 250 CIDR: 11.11.1.0/24

public-1

Auto-assign public IP

Enable

Firewall (security groups)

Create security group

Select existing security group

Security group name - required

vpc-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!\$*

Description - required

launch-wizard-16 created 2023-12-18T08:45:56.227Z

Auto assign public ip is disable in private subnet instances.

▼ Network settings

Info

VPC - required

Info

vpc-021081f1604067f96 (vpc-1)

11.11.0.0/16

↻

Subnet

Info

subnet-0d4294a4c225cb3bf

private-1

↻

Create new subnet

VPC: vpc-021081f1604067f96

Owner: 170303796048

Availability Zone: eu-north-1a

IP addresses available: 251

CIDR: 11.11.2.0/24)

Auto-assign public IP

Info

Disable

▼

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups

Info

Select security groups

▼

vpc-sg sg-05a05b6a2fc9e057e

✕

VPC: vpc-021081f1604067f96

↻

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

▼ Network settings

Info

VPC - required

Info

vpc-021081f1604067f96 (vpc-1)

11.11.0.0/16

↻

Subnet

Info

subnet-0bb8367d00d8f2527

private-2

↻

Create new subnet

VPC: vpc-021081f1604067f96

Owner: 170303796048

Availability Zone: eu-north-1a

IP addresses available: 251

CIDR: 11.11.3.0/24)

Auto-assign public IP

Info

Disable

▼

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups

Info

Select security groups

▼

vpc-sg sg-05a05b6a2fc9e057e

✕

VPC: vpc-021081f1604067f96

↻

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

▼ Network settings

Info

VPC - required

Info

vpc-021081f1604067f96 (vpc-1)

11.11.0.0/16

↻

Subnet

Info

subnet-0f52df4fa5788cddd

private-3

↻

Create new subnet

VPC: vpc-021081f1604067f96

Owner: 170303796048

Availability Zone: eu-north-1a

IP addresses available: 251

CIDR: 11.11.4.0/24)

Auto-assign public IP

Info

Disable

▼

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups

Info

Select security groups

▼

vpc-sg sg-05a05b6a2fc9e057e

✕

VPC: vpc-021081f1604067f96

↻

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

Instances (4) Info			Connect	Instance state ▼	Actions ▼	Launch instances ▼		
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>								1
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Pub
<input type="checkbox"/>	public-1	i-0394f268fc44178cb	Running	t3.micro	2/2 checks passed	No alarms	eu-north-1a	-
<input type="checkbox"/>	private-1	i-0105d0988b6915c6a	Running	t3.micro	2/2 checks passed	No alarms	eu-north-1a	-
<input type="checkbox"/>	private-2	i-09b3f63f61b71bd75	Running	t3.micro	2/2 checks passed	No alarms	eu-north-1a	-
<input type="checkbox"/>	private-3	i-04fdb157d95daeffa	Running	t3.micro	2/2 checks passed	No alarms	eu-north-1a	-

Connect to machine one check it has internet connectivity.

```
ubuntu@ip-11-11-1-234:~$ ping google.com
PING google.com (142.250.74.142) 56(84) bytes of data:
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=1 ttl=114 time=3.44 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=2 ttl=114 time=3.47 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=3 ttl=114 time=3.46 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=4 ttl=114 time=3.49 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=5 ttl=114 time=3.47 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=6 ttl=114 time=3.49 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 3.442/3.471/3.493/0.016 ms
ubuntu@ip-11-11-1-234:~$
```

i-0394f268fc44178cb (public-1)

PublicIPs: 13.49.72.148 PrivateIPs: 11.11.1.234

We cannot connect to private subnet instances directly so we can connect through SSH connection using the .pem key pair. For connecting the private 1 instance – go in public-1 instance – create a nano file aws_capstone_project1.pem paste the key inside the file then paste sudo chmod command and at last ssh-i-----2.9 command and connect .

EC2 > Instances > i-0105d0988b6915c6a > Connect to instance

Connect to instance Info

Connect to your instance i-0105d0988b6915c6a (private-1) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

i-0105d0988b6915c6a (private-1)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is aws_capstone_project1.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 `chmod 400 aws_capstone_project1.pem`
4. Connect to your instance using its Private IP:
 11.11.2.9

Example:

`ssh -i "aws_capstone_project1.pem" ubuntu@11.11.2.9`

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

```
ubuntu@ip-11-11-2-9:~$ ping google.com
PING google.com (216.58.211.14) 56(84) bytes of data.
64 bytes from arn09s20-in-f14.1e100.net (216.58.211.14): icmp_seq=1 ttl=53 time=3.52 ms
64 bytes from muc03s13-in-f14.1e100.net (216.58.211.14): icmp_seq=2 ttl=53 time=3.17 ms
64 bytes from arn09s20-in-f14.1e100.net (216.58.211.14): icmp_seq=3 ttl=53 time=3.18 ms
64 bytes from muc03s13-in-f14.1e100.net (216.58.211.14): icmp_seq=4 ttl=53 time=3.17 ms
64 bytes from muc03s13-in-f14.1e100.net (216.58.211.14): icmp_seq=5 ttl=53 time=3.23 ms
64 bytes from muc03s13-in-f14.1e100.net (216.58.211.14): icmp_seq=6 ttl=53 time=3.19 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 3.166/3.243/3.522/0.126 ms
ubuntu@ip-11-11-2-9:~$
```

i-0394f268fc44178cb (public-1)

PublicIPs: 13.49.72.148 PrivateIPs: 11.11.1.234

This time for connecting the private-2 machine we don't need to create nano file and paste chmod command .

```
ubuntu@ip-11-11-2-9:~$ exit
logout
Connection to 11.11.2.9 closed.
ubuntu@ip-11-11-1-234:~$ sudo ssh -i "aws_capstone_project1.pem" ubuntu@11.11.3.240
```

i-0394f268fc44178cb (public-1)

PublicIPs: 13.49.72.148 PrivateIPs: 11.11.1.234

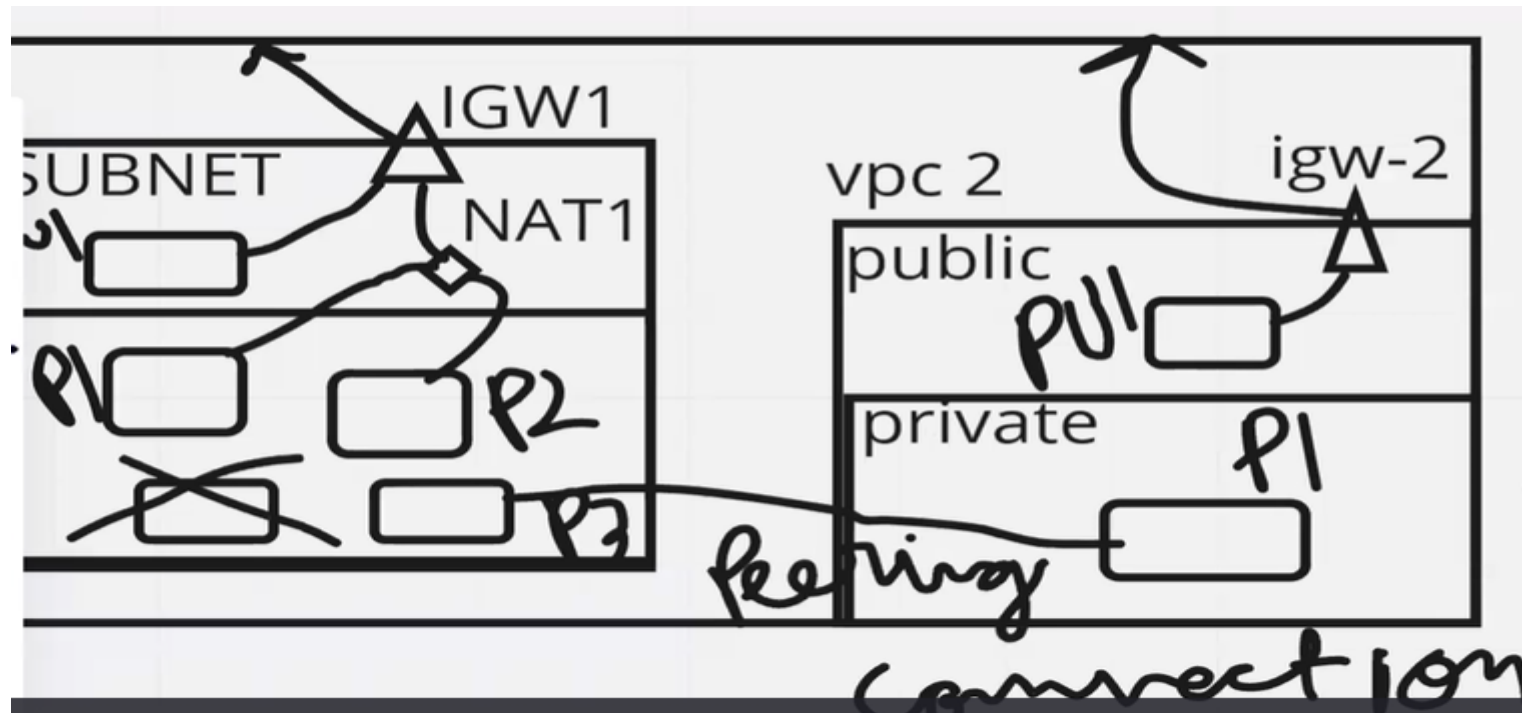
```

ubuntu@ip-11-11-3-240:~$ ping google.com
PING google.com (142.250.74.142) 56(84) bytes of data.
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=1 ttl=112 time=3.34 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=2 ttl=112 time=3.02 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=3 ttl=112 time=2.96 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=4 ttl=112 time=2.93 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=5 ttl=112 time=2.96 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.933/3.042/3.340/0.151 ms
ubuntu@ip-11-11-3-240:~$

```

i-0394f268fc44178cb (public-1)

PublicIPs: 13.49.72.148 PrivateIPs: 11.11.1.234



For development network we are going to follow the steps.

Name the Route table associated to this VPC.

Route tables (1/1) [Info](#)

Find resources by attribute or tag

Route table ID = rtb-03a5b9d0de669125e X Clear filters

< 1 > ⚙

<input checked="" type="checkbox"/>	Name ▾	Route table ID ▾	Explicit subnet associati... ▾	Edge associations ▾	Main ▾	VPC ▾
<input checked="" type="checkbox"/>	vpc-2-public	rtb-03a5b9d0de669125e	-	-	Yes	vpc-0c42de41e32e...

VPC > Route tables > Create route table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

vpc-2-no-int

VPC

The VPC to use for this route table.

vpc-0c42de41e32ec5c29 (vpc-2) ▾

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name X

Value - optional

Q vpc-2-no-int X

Remove

Add new tag

You can add 49 more tags.

Cancel

Create route table

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

vpc-2

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

12.12.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default ▾

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name X

Value - optional

Q vpc-2 X

Remove tag

Add tag

You can add 49 more tags.

Cancel

Create VPC

We need to create one more route table with no internet.

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

vpc-0c42de41e32ec5c29 (vpc-2)

Associated VPC CIDRs

IPv4 CIDRs

12.12.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

public

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

12.12.0.0/16

IPv4 subnet CIDR block

12.12.1.0/24

256 IPs

< > ^ v

▼ Tags - optional

Key

Q Name

X

Value - optional

Q public

X

Remove

Add new tag

You can add 49 more tags.

Remove

The next step is to create subnets.

Subnet 2 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

private

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

12.12.0.0/16

IPv4 subnet CIDR block

12.12.2.0/24

256 IPs

< > ^ v

▼ Tags - optional

Key

Q Name

X

Value - optional

Q private

X

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

vpc-2-igw

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name



Value - optional

Q vpc-2-igw



Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

In VPC-2-PUBLIC Route table edit route attach to igw-2.

Edit routes

Destination	Target	Status	Propagated
-------------	--------	--------	------------

12.12.0.0/16

local

Active

No

Q local



Q 0.0.0.0/0



Internet Gateway

-

No

Remove

Q igw-03ddd04d530b1b245



Add route

Cancel

Preview

Save changes

The following internet gateway was created: igw-03ddd04d530b1b245 - vpc-2-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC



igw-03ddd04d530b1b245 / vpc-2-igw

Actions

Details Info

Internet gateway ID

igw-03ddd04d530b1b245

State

Detached

VPC ID

-

Owner

170303796048

Tags

Manage tags

Q Search tags



1



Key

Value

Name

vpc-2-igw

Attach to VPC (igw-03ddd04d530b1b245) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

Q vpc-0c42de41e32ec5c29



AWS Command Line Interface command

Cancel

Attach internet gateway

In subnet association choose public subnet .

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (1)

Q Find subnet association

Name



Subnet ID



IPv4 CIDR

public

subnet-00086a540dae32f1c

12.12.1.0/24

In vpc-2-no-int Route table edit subnet association and private subnet.

VPC > Route tables > rtb-0849efb04a0d6058b > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

Name

Subnet ID

IPv4 CIDR

IPv6 CIDR

Route table ID

☐

public

subnet-00086a540dae32f1c

12.12.1.0/24–[rtb-03a5b9d0de669125e / vpc-2-publ](#)

☒

private

subnet-078f35e3e0a846876

12.12.2.0/24–[Main \(rtb-03a5b9d0de669125e / vpc-](#)

Selected subnets

subnet-078f35e3e0a846876 / private

Cancel

Save associations

Network settings

VPC - required

vpc-0c42de41e32ec5c29 (vpc-2)
12.12.0.0/16

Subnet

subnet-078f35e3e0a846876
VPC: vpc-0c42de41e32ec5c29
Availability Zone: eu-north-1a
Owner: 170303796048
IP addresses available: 251
CIDR: 12.12.2.0/24

private

Create new subnet

Auto-assign public IP

Disable

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Common security groups

Select security groups

vpc-2-sg sg-00d3d4cd5aa17ec3f
VPC: vpc-0c42de41e32ec5c29

Compare security group rules

Advanced network configuration

Network settings

VPC - required

vpc-0c42de41e32ec5c29 (vpc-2)
12.12.0.0/16

Subnet

subnet-00086a540dae32f1c
VPC: vpc-0c42de41e32ec5c29
Availability Zone: eu-north-1a
Owner: 170303796048
IP addresses available: 251
CIDR: 12.12.1.0/24

public

Create new subnet

Auto-assign public IP

Enable

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - required

vpc-2-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and .-:/()#,@!+=&[]!\$*

Description - required

launch-wizard-16 created 2023-12-18T10:23:11.577Z

Inbound Security Group Rules

Security group rule 1 (All, All, 0.0.0.0/0)

Remove

Type

All traffic

Protocol

All

Port range

All

Source type

Anywhere

Source

Add CIDR, prefix list or security
0.0.0.0/0

Description - optional

e.g. SSH for admin desktop

Launch two instances with these specifications.

Instances (6) [Info](#)

🔄

Connect

Instance state ▾

Actions ▾

Launch instances

▾

🔍

Find Instance by attribute or tag (case-sensitive)

<

1

>

⚙️

<input type="checkbox"/>	Name <div>✎</div> ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾	Pub
<input type="checkbox"/>	public-1	i-0394f268fc44178cb	✔️ Running <div>🔍 🔍</div>	t3.micro	✔️ 2/2 checks passed	No alarms +	eu-north-1a	–
<input type="checkbox"/>	private-1	i-0105d0988b6915c6a	✔️ Running <div>🔍 🔍</div>	t3.micro	✔️ 2/2 checks passed	No alarms +	eu-north-1a	–
<input type="checkbox"/>	private-2	i-09b3f63f61b71bd75	✔️ Running <div>🔍 🔍</div>	t3.micro	✔️ 2/2 checks passed	No alarms +	eu-north-1a	–
<input type="checkbox"/>	private	i-01ac860a5678a0fea	✔️ Running <div>🔍 🔍</div>	t3.micro	✔️ 2/2 checks passed	No alarms +	eu-north-1a	–
<input type="checkbox"/>	private-3	i-04fdb157d95daeffa	✔️ Running <div>🔍 🔍</div>	t3.micro	✔️ 2/2 checks passed	No alarms +	eu-north-1a	–
<input type="checkbox"/>	public	i-0c03dfd2de259f437	✔️ Running <div>🔍 🔍</div>	t3.micro	✔️ 2/2 checks passed	No alarms +	eu-north-1a	–

Select an instance

⚙️

✕

Let's connect to the public instance which has vpc-2 connection and check the internet connectivity.

```
ubuntu@ip-12-12-1-124:~$ ping google.com
PING google.com (142.250.74.46) 56(84) bytes of data.
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=1 ttl=55 time=2.88 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=2 ttl=55 time=2.91 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=3 ttl=55 time=2.93 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=4 ttl=55 time=2.92 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=5 ttl=55 time=2.93 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=6 ttl=55 time=2.93 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=7 ttl=55 time=2.97 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=8 ttl=55 time=3.01 ms
^C
--- google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 2.880/2.935/3.012/0.037 ms
ubuntu@ip-12-12-1-124:~$
```

i-0c03dfd2de259f437 (public)

PublicIPs: 13.53.93.143 PrivateIPs: 12.12.1.124

Now it's time to create peering connection .

Peering connections

Info

Find resources by attribute or tag

Actions

Create peering connection

Name

Peering connection ID

Status

Requester VPC

Acceptor VPC

No peering connection found

VPC

Peering connections

Create peering connection

Create peering connection

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately.

Info

Peering connection settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

vpc1-vpc2-pc

Select a local VPC to peer with

VPC ID (Requester)

vpc-021081f1604067f96 (vpc-1)

VPC CIDRs for vpc-021081f1604067f96 (vpc-1)

CIDR	Status	Status reason
11.11.0.0/16	Associated	-

Select another VPC to peer with

Account

My account

Another account

Region

This Region (eu-north-1)

Another Region

VPC ID (Acceptor)

vpc-0c42de41e32ec5c29 (vpc-2)

VPC CIDRs for vpc-0c42de41e32ec5c29 (vpc-2)

CIDR	Status	Status reason
12.12.0.0/16	Associated	-

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Name

Value - optional

vpc1-vpc2-pc

Remove

Add new tag

You can add 49 more tags.

Cancel

Create peering connection

Choose the peering connection and accept the request.

Peering connections (1/1) [Info](#)

Name

Peering connection ID

Status

Requester VPC

vpc1-vpc2-pc

pcx-0be3330a21bf6b022

Pending acceptance

Accept request

Reject request

Edit DNS settings

Manage tags

Delete peering connection

Go in vpc-1-no-int Route table – edit route –save changes.

VPC > Route tables > rtb-0d0c884a471cc2db3 > Edit routes

Edit routes

Destination	Target	Status	Propagated
11.11.0.0/16	<div>local</div> <div><input type="text" value="local"/></div>	<div>Active</div>	No
<div><input type="text" value="12.12.0.0/16"/></div>	<div>Peering Connection</div> <div><input type="text" value="pcx-"/></div>	-	No <div>Remove</div>

Add route

Cancel

Preview

Save changes

Also do the same with vpc-2-no-int Route table.

VPC > Route tables > rtb-0849efb04a0d6058b > Edit routes

Edit routes

Destination	Target	Status	Propagated
12.12.0.0/16	<div>local</div> <div>Q local</div>	✔ Active	No
<div>Q 11.11.0.0/16</div>	<div>Peering Connection</div> <div>Q pcx-0be3330a21bf6b022</div>	-	No <div>Remove</div>

Add route

Cancel

Preview

Save changes

For connecting the private subnet instance these steps need to follow .

```
ubuntu@ip-12-12-1-124:~$ sudo nano aws_capstone_project1.pem
ubuntu@ip-12-12-1-124:~$ sudo chmod 400 aws_capstone_project1.pem
ubuntu@ip-12-12-1-124:~$ sudo ssh -i "aws_capstone_project1.pem" ubuntu@12.12.2.215
```

i-0c03dfd2de259f437 (public)

PublicIPs: 13.53.93.143 PrivateIPs: 12.12.1.124

This private subnet instance is not get updated because it doesn't have NAT gateway. But for testing it have a peering connection we need to copy the ip of private3 instance and paste that in private instance .

```
ubuntu@ip-12-12-2-215:~$ ping 11.11.4.232
PING 11.11.4.232 (11.11.4.232) 56(84) bytes of data.
64 bytes from 11.11.4.232: icmp_seq=1 ttl=64 time=0.375 ms
64 bytes from 11.11.4.232: icmp_seq=2 ttl=64 time=0.207 ms
64 bytes from 11.11.4.232: icmp_seq=3 ttl=64 time=0.158 ms
64 bytes from 11.11.4.232: icmp_seq=4 ttl=64 time=0.149 ms
64 bytes from 11.11.4.232: icmp_seq=5 ttl=64 time=0.207 ms
64 bytes from 11.11.4.232: icmp_seq=6 ttl=64 time=0.179 ms
64 bytes from 11.11.4.232: icmp_seq=7 ttl=64 time=0.154 ms
^C
--- 11.11.4.232 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6128ms
rtt min/avg/max/mdev = 0.149/0.204/0.375/0.073 ms
ubuntu@ip-12-12-2-215:~$
```

i-0c03dfd2de259f437 (public)

PublicIPs: 13.53.93.143 PrivateIPs: 12.12.1.124