

You work for XYZ Corporation, and based on the expansion requirements of your company, you have been asked to create and setup distinct Amazon VPCs for production and development teams.

You are expected to perform the following tasks for the respective VPCs:

For the production network:

1. Design and build a four-tier architecture
2. Create five subnets. Among them, four should be private with names app1, app2, dbcache, and db, and the fifth one should be public with the name web
3. Launch instances in all subnets, and name them as per the subnet as they are launched in
4. Allow the dbcache instance and the app1 subnet to send Internet requests
5. Manage security groups and NACLs
6. Create a VPC Endpoint for the S3 service, and access the objects in any bucket from within the VPC

For the development network:

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

← → ↻ <https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#vpcs:> ☆

Error occurred, please reload.

VPC dashboard

EC2 Global View

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs (2)

Search

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	-	vpc-026bee67a18a8c8c4	Available	172.31.0.0/16
<input type="checkbox"/>	prod-VPC	vpc-085759cf29b6d37bf	Available	10.20.0.0/16

VPC dashboard

EC2 Global View

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Subnets (11)

Find resources by attribute or tag

<input type="checkbox"/>	Name	Subnet ID	State	VPC
<input type="checkbox"/>	-	subnet-06637099d06f4ac3d	Available	vpc-026bee67a18a8c8c4
<input type="checkbox"/>	-	subnet-0b3183a353211ec71	Available	vpc-026bee67a18a8c8c4
<input type="checkbox"/>	-	subnet-04f55171486f56060	Available	vpc-026bee67a18a8c8c4
<input type="checkbox"/>	-	subnet-02eeb0c6f902fe3e0	Available	vpc-026bee67a18a8c8c4
<input type="checkbox"/>	-	subnet-054b178e698829249	Available	vpc-026bee67a18a8c8c4
<input type="checkbox"/>	-	subnet-03bd8e82576424237	Available	vpc-026bee67a18a8c8c4
<input type="checkbox"/>	dbcache	subnet-093aedd71c4454cc0	Available	vpc-085759cf29b6d37bf
<input type="checkbox"/>	app2	subnet-034e64dc8262c9a16	Available	vpc-085759cf29b6d37bf
<input type="checkbox"/>	db	subnet-035ab55c0401892c4	Available	vpc-085759cf29b6d37bf
<input type="checkbox"/>	web	subnet-04dd1b80a2f4dca49	Available	vpc-085759cf29b6d37bf
<input type="checkbox"/>	app1	subnet-0e3158e240928531c	Available	vpc-085759cf29b6d37bf

TO MAKE PUBLIC SUBNET PUBLIC: edit subnet setting by Auto-assign IP settings

[VPC](#) > [Subnets](#) > [subnet-04dd1b80a2f4dca49](#) > Edit subnet settings

Edit subnet settings

Subnet

Subnet ID	Name
subnet-04dd1b80a2f4dca49	web

Auto-assign IP settings

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

CREATE ROUTE-TABLE: ASS THE VPC CREATED WITH IT

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.

RTABLE

VPC

The VPC to use for this route table.

vpc-085759cf29b6d37bf (prod-VPC)

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 X

Q RTABLE X

Remove

VPC dashboard

EC2 Global View

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

Internet gateways (2)

Info

Search

Actions

Create internet gateway

	Name	Internet gateway ID	State	VPC ID
<input type="checkbox"/>	-	igw-0fb3d0d1c5709f38f	Attached	vpc-026b
<input type="checkbox"/>	IGW1	igw-0792a4e12ea3c3d43	Detached	-

VPC > Internet gateways > Attach to VPC (igw-0792a4e12ea3c3d43)

Attach to VPC (igw-0792a4e12ea3c3d43)

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-085759cf29b6d37bf X

AWS Command Line Interface command

Cancel

Attach internet gateway

ASSOCIATE IGW with route table created

VPC > Route tables > rtb-0e371b350d6a6ad73 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.20.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	-	No

local

Internet Gateway

igw-0792a4e12ea3c3d43

Add route

Cancel

Preview

Save

ASSOCIATE ONLY PUBLIC SUBNET TO THE RT

VPC > Route tables > rtb-0e371b350d6a6ad73 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/5)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	dbcache	subnet-093aedd71c4454cc0	10.20.3.0/24	-	Main (rtb-06069d42e7142eed7)
<input type="checkbox"/>	app2	subnet-034e64dc8262c9a16	10.20.2.0/24	-	Main (rtb-06069d42e7142eed7)
<input type="checkbox"/>	db	subnet-035ab55c0401892c4	10.20.4.0/24	-	Main (rtb-06069d42e7142eed7)
<input checked="" type="checkbox"/>	web	subnet-04dd1b80a2f4dca49	10.20.5.0/24	-	Main (rtb-06069d42e7142eed7)
<input type="checkbox"/>	app1	subnet-0e3158e240928531c	10.20.1.0/24	-	Main (rtb-06069d42e7142eed7)

Selected subnets

subnet-04dd1b80a2f4dca49 / web

Cancel

Save associations

VPC dashboard

EC2 Global View

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

You have successfully updated subnet associations for rtb-0e371b350d6a6ad73 / RTABLE.

VPC > Route tables > rtb-0e371b350d6a6ad73

rtb-0e371b350d6a6ad73 / RTABLE

Actions

Details Info

Route table ID rtb-0e371b350d6a6ad73	Main No	Explicit subnet associations subnet-04dd1b80a2f4dca49 / web	Edge associations -
VPC vpc-085759cf29b6d37bf prod-VPC	Owner ID 051875392745		

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (1)

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
web	subnet-04dd1b80a2f4dca49	10.20.5.0/24	-

Edit subnet associations

Now five subnets are created. app1, app2, dbcache, and db are private, and the fifth one: web is public.

3. Launch instances in all subnets, and name them as per the subnet as they are launched in

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Instances (5) Info

Find Instance by attribute or tag (case-sensitive)

All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
dbcache	i-02ad7790f8de07c2a	Running	t2.micro	2/2 checks passed	View alarms	us-east-1
app1	i-063af40e0bb17705b	Running	t2.micro	2/2 checks passed	View alarms	us-east-1
app2	i-071556baf21e7558d	Running	t2.micro	2/2 checks passed	View alarms	us-east-1
db	i-0c4d052ae8ac5cf0c	Running	t2.micro	Initializing	View alarms	us-east-1
web	i-01e90ba2dfd57c043	Running	t2.micro	2/2 checks passed	View alarms	us-east-1

Select an instance

4. Allow the dbcache instance and the app1 subnet to send Internet requests

The private instance in the private subnets need NATgateway to be able to have access to internet.

1: CREATE PRIVATE RT

Route tables	<input type="checkbox"/>	RT-PRIVATE	rtb-000e1e86533caa362	-	-	No
--------------	--------------------------	------------	---------------------------------------	---	---	----

ASSOCIATE PRIVATE SUBNETS TO IT

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (4/5)

Filter subnet associations

☒

dbcache

[subnet-093aedd71c4454cc0](#)

10.20.3.0/24

-

[Main \(rtb-06069d42e7142eed7\)](#)

☒

app2

[subnet-034e64dc8262c9a16](#)

10.20.2.0/24

-

[Main \(rtb-06069d42e7142eed7\)](#)

☐

web

[subnet-04dd1b80a2f4dca49](#)

10.20.5.0/24

-

[rtb-0e371b350d6a6ad73 / RTABL](#)

☒

db

[subnet-0178897502691a38a](#)

10.20.4.0/24

-

[Main \(rtb-06069d42e7142eed7\)](#)

☒

app1

[subnet-0e3158e240928531c](#)

10.20.1.0/24

-

[Main \(rtb-06069d42e7142eed7\)](#)

Selected subnets

subnet-093aedd71c4454cc0 / dbcache X

subnet-034e64dc8262c9a16 / app2 X

subnet-0178897502691a38a / db X

subnet-0e3158e240928531c / app1 X

Cancel Save associations

CREATE NAT-gateway

-- pick public subnet

-- EIP allocate

Elastic IP address 52.200.213.223 (elipalloc-08b7cef72faaf3b57) allocated.

NAT gateway settings

Name - optional

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

NATgateway

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

subnet-04dd1b80a2f4dca49 (web)

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.

elipalloc-08b7cef72faaf3b57

Allocate Elastic IP

Additional settings [Info](#)

In Private RT: edit and pit NAT-gateway

VPC > Route tables > rtb-000e1e86533caa362 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.20.0.0/16	local	Active	No
0.0.0.0/0	NAT Gateway	-	No
	nat-0e00ee4cfddfbfb4		

TEST 'web' instances

```
subby@subby-ubuntu:~/documents$ ssh -t -i newkey-vmgthta.pem ubuntu@34.204.61.230
The authenticity of host '34.204.61.230 (34.204.61.230)' can't be established.
ED25519 key fingerprint is SHA256:YAdHvSUPzPWfotNGfp29Gh0R94NyODEFSmSn+mnrH2A.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.204.61.230' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1014-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro
```

```
ubuntu@ip-10-20-5-123:~$ sudo ping aws.com
PING aws.com (99.84.108.3) 56(84) bytes of data.
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
1 ttl=245 time=0.780 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
2 ttl=245 time=0.789 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
3 ttl=245 time=0.845 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
4 ttl=245 time=0.836 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
5 ttl=245 time=0.864 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
6 ttl=245 time=0.898 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
7 ttl=245 time=0.828 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
8 ttl=245 time=0.914 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
9 ttl=245 time=0.899 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
10 ttl=245 time=0.828 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
11 ttl=245 time=0.828 ms
10.0.0.0/8 is on the subnet (subby-pub-instance)
PublicIPs: 18.206.81.213 PrivateIPs: 20.0.1.228
```

4. Allow the dbcache instance and the app1 subnet to send Internet requests

~/Documents: being location of keypair on my local pc

```
scp -i ~/Documents/newkey-virginia.pem ~/Documents/newkey-virginia.pem
ubuntu@34.204.61.230:/home/ubuntu/newkey-virginia.pem
```

scp (secure copy) command to securely transfer the private key file from local device to the instance.

```
ssh -i ~/Documents/newkey-virginia.pem ubuntu@34.204.61.230 : public ip
```

After running this command, the private key file should be securely transferred to the specified location on the remote instance.

```
ssh -i /home/ubuntu/newkey-virginia.pem ubuntu@10.20.1.211 : private ip
```



```

ubuntu@ip-10-20-1-211:~$ sudo ping aws.com
PING aws.com (99.84.108.37) 56(84) bytes of data.
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=1 ttl=243 time=1.68 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=2 ttl=243 time=1.47 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=3 ttl=243 time=1.40 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=4 ttl=243 time=1.46 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=5 ttl=243 time=1.41 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=6 ttl=243 time=1.40 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=7 ttl=243 time=1.60 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=8 ttl=243 time=1.51 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=9 ttl=243 time=1.46 ms

```

OR

EC2 Instance Connect to Public instance and from there; ssh into private instance.

`ssh -i newkey-virginia.pem ubuntu@10.20.1.211 :..... private ip`

app1 server

```

ubuntu@ip-10-20-5-123:~$ ssh -i newkey-virginia.pem ubuntu@10.20.1.211
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1014-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Fri Apr 19 20:02:13 UTC 2024

System load:  0.0               Processes:           98
Usage of /:   20.7% of 7.57GB   Users logged in:    1

```

```

ubuntu@ip-10-20-1-211:~$ sudo ping aws.com
PING aws.com (99.84.108.3) 56(84) bytes of data.
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=1 ttl=244 time=1.65 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=2 ttl=244 time=1.53 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=3 ttl=244 time=1.43 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=4 ttl=244 time=1.42 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=5 ttl=244 time=1.42 ms
^C
--- aws.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.421/1.489/1.645/0.088 ms

```

dbcache server

```
ubuntu@ip-10-20-5-123:~$ ssh -i newkey-virginia.pem ubuntu@10.20.3.244
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1014-aws x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro
```

```
System information as of Fri Apr 19 20:19:44 UTC 2024
```

```
System load:  0.0          Processes:           97
Usage of /:   20.4% of 7.57GB Users logged in:      0
```

```
ubuntu@ip-10-20-3-244:~$ sudo ping google.com
```

```
PING google.com (172.253.122.139) 56(84) bytes of data.
```

```
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=1 ttl=101 time=2.99 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=2 ttl=101 time=2.76 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=3 ttl=101 time=2.66 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=4 ttl=101 time=2.66 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=5 ttl=101 time=2.70 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=6 ttl=101 time=2.81 ms
c64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=7 ttl=101 time=2.66 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=8 ttl=101 time=2.77 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=9 ttl=101 time=2.71 ms
```

For the development network:

1. Design and build a two-tier architecture with two subnets named web and db, and launch instances in both subnets, naming them as per the subnet names

DEV-VPC

Your VPCs (3) Info						Refresh	Actions	Create VPC
<input type="text" value="Search"/>						< 1 > Settings		
<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR				
<input type="checkbox"/>	-	vpc-026bee67a18a8c8c4	Available	172.31.0.0/16				
<input type="checkbox"/>	prod-VPC	vpc-085759cf29b6d37bf	Available	10.20.0.0/16				
<input type="checkbox"/>	dev-VPC	vpc-03889b0865f619f61	Available	30.10.0.0/16				

2SUBNETS: WEB AND DB

Subnets (2) Info						Refresh	Actions	Create subnet
<input type="text" value="Find resources by attribute or tag"/>						< 1 > Settings		
<div><div>dev-</div><div>X</div><div>Clear filters</div></div>								
<input type="checkbox"/>	Name	Subnet ID	State	VPC				
<input type="checkbox"/>	dev-web	subnet-063ed1e692e1f3771	Available	vpc-03889b0865f619f61 dev-...				
<input type="checkbox"/>	dev-db	subnet-0d76436399c29f04d	Available	vpc-03889b0865f619f61 dev-...				

AUTO ASSIGN IP TO THE PUB SUBNET

[VPC](#) > [Subnets](#) > [subnet-063ed1e692e1f3771](#) > Edit subnet settings

Edit subnet settings [Info](#)

Subnet

Subnet ID	Name
subnet-063ed1e692e1f3771	dev-web

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](#)

CREATE IGW

✓ You have successfully changed subnet settings:

- Enable auto-assign public IPv4 address

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.

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="IGW-DEV"/>	<input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>		

You can add 49 more tags.

ATTACH IGW TO VPC

[VPC](#) > [Internet gateways](#) > Attach to VPC (igw-014b62adec710f892)

Attach to VPC (igw-014b62adec710f892) [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.

CREATE RT

& edit RT and pick target as igw

VPC > Route tables > rtb-076ae6b5578971c09 > Edit routes

Edit routes

Destination	Target	Status	Propagated
30.10.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	-	No

Add route

RT association with public subnet

VPC > Route tables > rtb-076ae6b5578971c09 > 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
<input checked="" type="checkbox"/>	dev-web	subnet-063ed1e692e1f3771	30.10.1.0/24	-	Main (rtb-0f4ee8b617767c669)
<input type="checkbox"/>	dev-db	subnet-0d76436399c29f04d	30.10.2.0/24	-	Main (rtb-0f4ee8b617767c669)

Selected subnets

subnet-063ed1e692e1f3771 / dev-web

Cancel Save associations

VPC dashboard

EC2 Global View

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

You have successfully updated subnet associations for rtb-076ae6b5578971c09 / dev-pub-RT.

Details

Route table ID

rtb-076ae6b5578971c09

VPC

vpc-03889b0865f619f61 | dev-VPC

Main

No

Owner ID

051875392745

Explicit subnet associations

subnet-063ed1e692e1f3771 / dev-web

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	lgw-014b62adec710f892	Active	No
30.10.0.0/16	local	Active	No

launch instances in both subnets, naming them as per the subnet names

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Instances

Instances

Instance Types

Instances (2) Info

Find Instance by attribute or tag (case-sensitive)

All states

dev- Clear filters

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Avai
<input type="checkbox"/>	dev-web	i-0ac5b261fbe6abcc0	Running	t2.micro	Initializing	View alarms	us-e
<input type="checkbox"/>	dev-db	i-099b9eac29a571902	Pending	t2.micro	-	View alarms	us-e

dev-web instance can access internet

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-30-10-1-123:~$ sudo ping google.com
PING google.com (172.253.115.138) 56(84) bytes of data.
64 bytes from bg-in-f138.1e100.net (172.253.115.138): icmp_seq=1 ttl=58 time=2.34 ms
64 bytes from bg-in-f138.1e100.net (172.253.115.138): icmp_seq=2 ttl=58 time=2.34 ms
64 bytes from bg-in-f138.1e100.net (172.253.115.138): icmp_seq=3 ttl=58 time=2.31 ms
64 bytes from bg-in-f138.1e100.net (172.253.115.138): icmp_seq=4 ttl=58 time=2.35 ms
64 bytes from bg-in-f138.1e100.net (172.253.115.138): icmp_seq=5 ttl=58 time=2.35 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 2.307/2.336/2.350/0.015 ms
ubuntu@ip-30-10-1-123:~$
```

i-0ac5b261fbe6abcc0 (dev-web)

PublicIPs: 52.70.130.235 PrivateIPs: 30.10.1.123

dev-db can not access internet (not even when ssh from public instance)NATgateway was not created

```
ubuntu@ip-30-10-1-123:~$ ssh -i newkey-virginia.pem ubuntu@30.10.2.147
Warning: Identity file newkey-virginia.pem not accessible: No such file or directory.
The authenticity of host '30.10.2.147 (30.10.2.147)' can't be established.
ED25519 key fingerprint is SHA256:uhcQHdKcpWJQn5J3QG5uNWPVe/sC5jd8ZPYyd1S7110.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '30.10.2.147' (ED25519) to the list of known hosts.
ubuntu@30.10.2.147: Permission denied (publickey).
ubuntu@ip-30-10-1-123:~$
```

i-0ac5b261fbe6abcc0 (dev-web)

PublicIPs: 52.70.130.235 PrivateIPs: 30.10.1.123

3. Create a peering connection between the production network and the development network

CREATE PEERING CONNECTION BETWEEN PROD-VPC AND DEV-VPC

Select a local VPC to peer with

VPC ID (Requester)
vpc-085759cf29b6d37bf (prod-VPC)

VPC CIDRs for vpc-085759cf29b6d37bf (prod-VPC)

CIDR	Status	Status reason
10.20.0.0/16	Associated	-

Select another VPC to peer with

Account
☒ My account
☐ Another account

Region
☒ This Region (us-east-1)
☐ Another Region

VPC ID (Acceptor)
vpc-03889b0865f619f61 (dev-VPC)

VPC CIDRs for vpc-03889b0865f619f61 (dev-VPC)

VPC dashboard

EC2 Global View

Filter by VPC:
Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

A VPC peering connection pcx-04d6f454f01a1e268 / Peering has been requested.

VPC > Peering connections > pcx-04d6f454f01a1e268

pcx-04d6f454f01a1e268 / Peering

Pending acceptance

You can accept or reject this peering connection request using the 'Actions' menu. You have until Friday, April 2 GMT+1 to accept or reject the request, otherwise it expires.

Details

Info

Actions

Accept request

Reject request

Edit DNS settings

Manage tags

Delete peering connection

EDIT RT OF THE VPC

PUBLIC RT VPC2 I.e dev

cidr of vpc1 ----- pcx

VPC > Route tables > rtb-076ae6b5578971c09 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
30.10.0.0/16	local	Active	No	
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="local"/>			
	Internet Gateway	Active	No	Remove
	<input type="text" value="igw-014b62adec710f892"/>			
<input type="text" value="10.20.0.0/16"/>	Peering Connection	-	No	Remove
	<input type="text" value="pcx-04d6f454f01a1e268"/>			
<input type="button" value="Add route"/>				

PRIVATE RT OF VPC1 I.e production

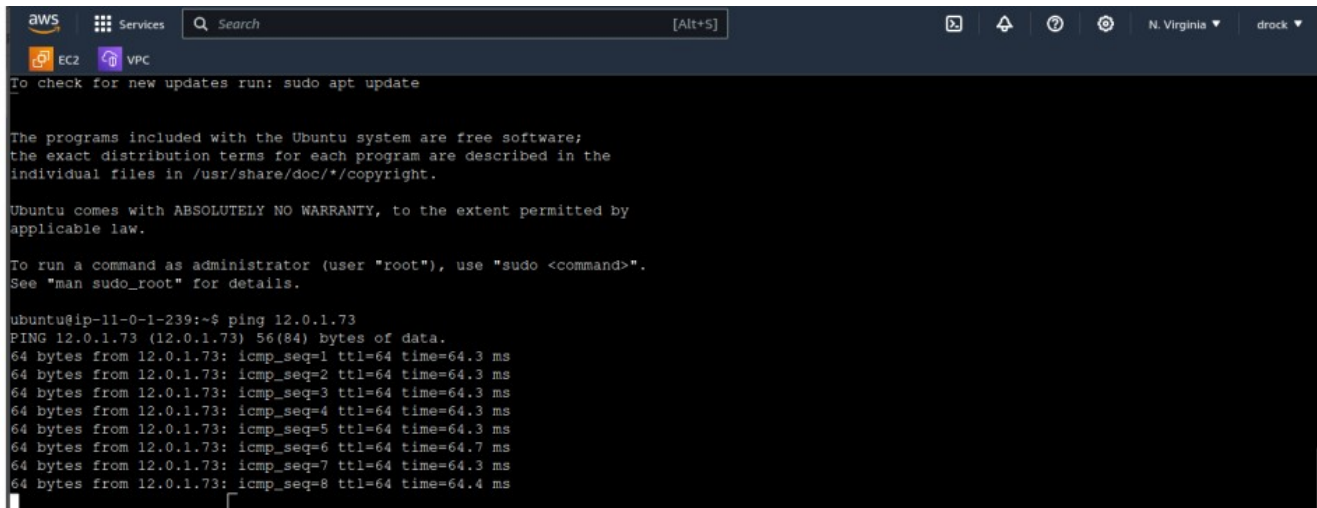
cidr of vpc1 ----- pcx

VPC > Route tables > rtb-000e1e86533caa362 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
10.20.0.0/16	local	Active	No	
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="local"/>			
	NAT Gateway	Active	No	Remove
	<input type="text" value="nat-0e0ee4cfddfbfbf4"/>			
<input type="text" value="30.10.0.0/16"/>	Peering Connection	-	No	Remove
	<input type="text" value="pcx-04d6f454f01a1e268"/>			
<input type="button" value="Add route"/>				

NOW, connect to public instance of a VPC and from their attempt to connect to private instance of another VPC / ping private instance from public instances



The screenshot shows an AWS console terminal window. The top bar includes the AWS logo, 'Services' menu, a search bar, and navigation icons. Below the bar, there are tabs for 'EC2' and 'VPC'. The terminal content shows a series of system messages and a successful ping command. The messages include instructions on how to update the system and run commands as administrator. The ping command is executed from a user 'ubuntu' on an instance with IP 'ip-11-0-1-239', targeting the IP '12.0.1.73'. The output shows 8 successful ping requests with varying response times.

```
aws Services [Alt+S]
EC2 VPC
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-11-0-1-239:~$ ping 12.0.1.73
PING 12.0.1.73 (12.0.1.73) 56(84) bytes of data.
64 bytes from 12.0.1.73: icmp_seq=1 ttl=64 time=64.3 ms
64 bytes from 12.0.1.73: icmp_seq=2 ttl=64 time=64.3 ms
64 bytes from 12.0.1.73: icmp_seq=3 ttl=64 time=64.3 ms
64 bytes from 12.0.1.73: icmp_seq=4 ttl=64 time=64.3 ms
64 bytes from 12.0.1.73: icmp_seq=5 ttl=64 time=64.3 ms
64 bytes from 12.0.1.73: icmp_seq=6 ttl=64 time=64.7 ms
64 bytes from 12.0.1.73: icmp_seq=7 ttl=64 time=64.3 ms
64 bytes from 12.0.1.73: icmp_seq=8 ttl=64 time=64.4 ms
```