

AMAZON VPC



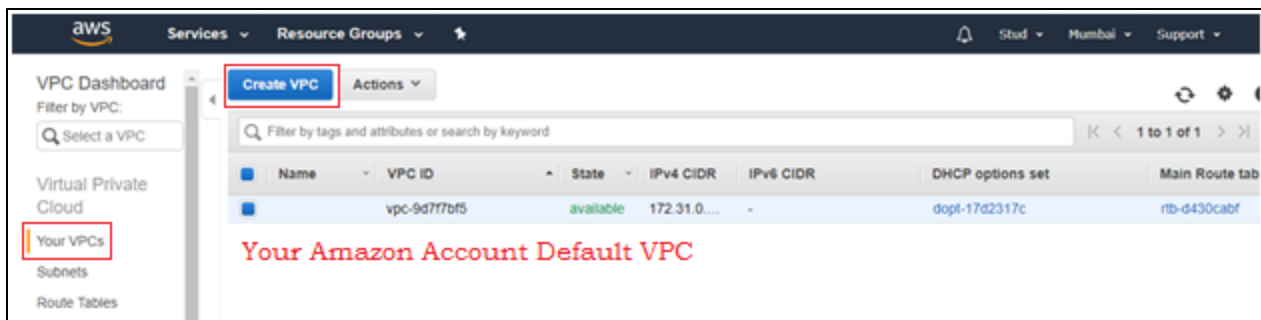
Virtual Private Cloud

Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network which is defined by you. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS. The list of AWS services that can be used with Amazon VPC are mention below,

1. Amazon EC2
2. Amazon Route 53
3. Amazon WorkSpaces
4. Auto Scaling
5. Elastic Load Balancing
6. AWS Data Pipeline
7. Elastic Beanstalk
8. Amazon Elastic Cache
9. Amazon EMR
10. Amazon OpsWorks
11. Amazon RDS
12. Amazon Redshift

Steps to create and configure VPC, Subnet, Internet Gateway and Route Table:

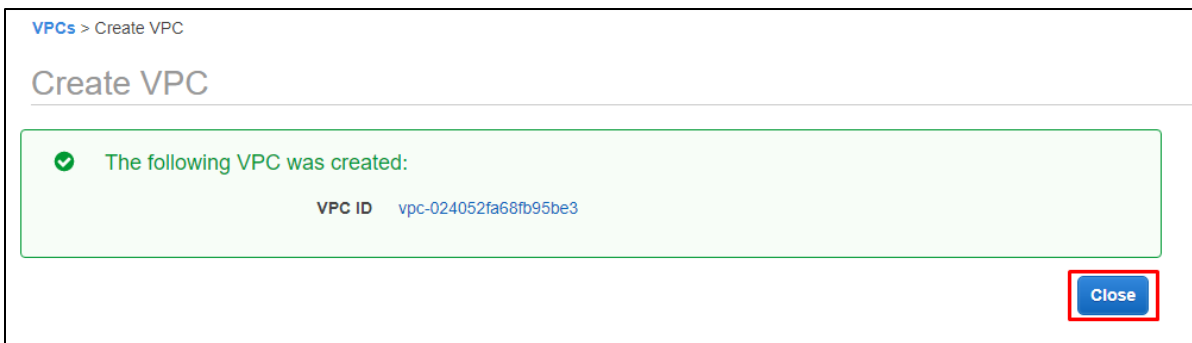
1. Open the Amazon Web Console and in Services search for VPC or scroll down and look for Networking & Content Delivery below VPC will be displayed
2. A default VPC will be automatically created during the account creation. On the top search and select Create VPC a new page will open



3. Fill the necessary details to create VPC and please mention the CIDR value correctly based on your requirements

The screenshot shows the 'Create VPC' form. The 'Name tag' field contains 'Custom_VPC'. The 'IPv4 CIDR block*' field contains '10.0.0.0/16'. The 'IPv6 CIDR block' section has 'No IPv6 CIDR Block' selected. The 'Tenancy' dropdown is set to 'Default'. At the bottom right, the 'Create' button is highlighted with a red box. A legend at the bottom left indicates '* Required'.

4. A confirmation page will open with VPC ID



5. Compare the Amazon VPC and custom created VPC

Create VPC Actions

Filter by tags and attributes or search by keyword

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
Custom_VPC	vpc-024052fa68fb95be3	available	10.0.0.0/16	-	dopt-17d2317c
aws_VPC	vpc-9d7f7bf5	available	172.31.0.0/16	-	dopt-17d2317c

VPC: vpc-9d7f7bf5 Amazon default VPC

Description CIDR Blocks Flow Logs Tags

VPC ID: vpc-9d7f7bf5
 State: available
 IPv4 CIDR: 172.31.0.0/16
 DNS resolution: Enabled
 DNS hostnames: Enabled
 Route table: rtb-d430cabf

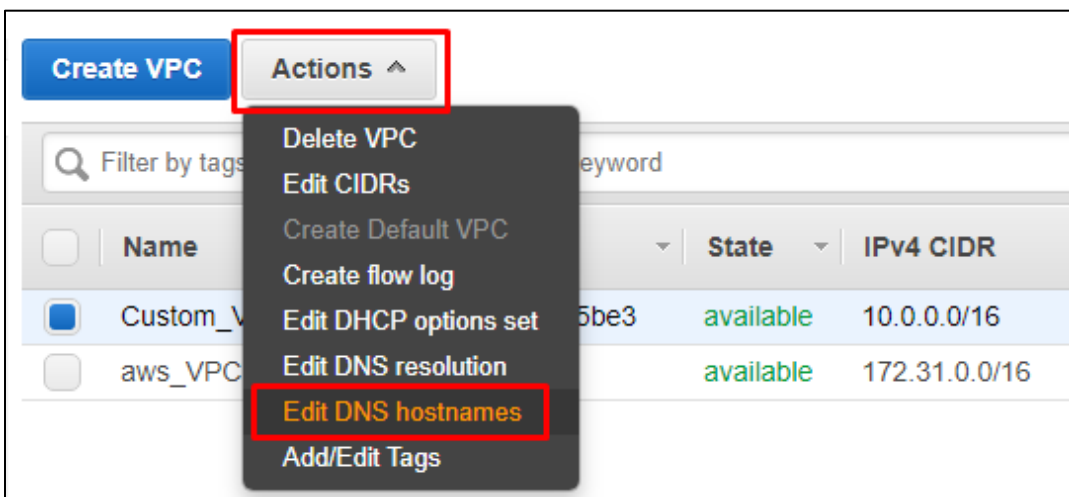
Tenancy: default
 Default VPC: Yes
 IPv6 CIDR: -
 Network ACL: acl-49f01f22
 DHCP options set: dopt-17d2317c
 Owner: 393106192112

VPC: vpc-024052fa68fb95be3 Custom created VPC

VPC ID: vpc-024052fa68fb95be3
 State: available
 IPv4 CIDR: 10.0.0.0/16
 DNS resolution: Enabled
 DNS hostnames: Disabled
 Route table: rtb-08d29780878c649d3

Tenancy: default
 Default VPC: No
 IPv6 CIDR: -
 Network ACL: acl-061e7599e0114ae09
 DHCP options set: dopt-17d2317c
 Owner: 393106192112

6. Select the custom VPC and click on Action to enable the DNS hostnames



7. It will open a new page and select the box to enable the DNS Hostnames

VPCs > Edit DNS hostnames

Edit DNS hostnames

VPC ID vpc-024052fa68fb95be3

DNS hostnames ☒ enable *Select to check the box*

* Required

Cancel **Save**

8. Once it done it will display the DNS Hostname has been updated and in the Description the DNS Hostnames will be Enabled but do not change the custom VPC to default under no circumstances

VPCs > Edit DNS hostnames

Edit DNS hostnames

✔ DNS hostnames updated

Close

9. To create new Gateway click on the Create Internet Gateway on the top let around the corner

Create internet gateway Actions ▾

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name ▾	ID ▾	State	VPC ▾	Owner
<input checked="" type="checkbox"/>	Amazon_IGW	igw-7f36e017	attached	vpc-9d7f7bf5 aw...	

10. It will open a new page and enter the name of your choice and click on create

Internet gateways > Create internet gateway

Create internet gateway

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.

Name tag ⓘ

* Required

Cancel **Create**

11. It will navigate to the page where the Internet Gateway id is generated and select close

Internet gateways > Create internet gateway

Create internet gateway

✓ The following internet gateway was created:

Internet gateway ID [igw-0f2646868fed174a2](#)

[Close](#)

12. Once the IGW has been created it will detached status and need to be connected with VPC

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	ID	State	VPC	Owner
<input checked="" type="checkbox"/>	Custom_IGW	igw-0f2646868fed...	detached	-	
<input type="checkbox"/>		igw-7f36e017	attached	vpc-9d7f7bf5 aw...	

13. Click on the Action option and select Attach to VPC

Create internet gateway

Actions ^

Filter by tags and attributes

Delete internet gateway

Attach to VPC

Detach from VPC

Add/Edit Tags

<input type="checkbox"/>	Name	ID	State	VPC	Owner
<input checked="" type="checkbox"/>	Custom_IGW	igw-0f2646868fed...	detached	-	
<input type="checkbox"/>		igw-7f36e017	attached	vpc-9d7f7bf5 aw...	

14. Enter the VPC id or click so it can list the numbers of VPC created so far and select Attach the status will be changed to attached

Internet gateways > Attach to VPC

Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC*

► AWS Command Line

VPC ID	Name
vpc-024052fa68fb95be3	Custom_VPC

* Required

[Cancel](#) [Attach](#)

15. On the left side select Subnets to navigate to the page and create subnet and select the Create Subnet button to begin the process
16. Fill the details correctly and Create Public Subnet even slight mistake Subnet cannot be created

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag ⓘ

VPC* ⓘ Enter the VPC name or a Filter window will open you can select it from there

Vpc-9d7f7bf5	aws_VPC
Vpc-02405fa68fb95be3	Custom_VPC

Availability Zone ⓘ Zone is **optional** select it if required or automatically it will select a zone during the Instance creation

Name	ID
No preference	
ap-south-1a	aps1-az1
ap-south-1b	aps1-az3
ap-south-1c	aps1-az2

IPv4 CIDR block* ⓘ

* Required

Cancel **Create**

17. If the Subnet is successfully created a subnet id will be generated in next page

Subnets > Create subnet

Create subnet

✓ The following Subnet was created:

Subnet ID `subnet-0c9ca43876816e0a0`

Close

18. Create the Private Subnet

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC*

VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	

Availability Zone

IPv4 CIDR block* Range of the IPV4

* Required

[Cancel](#) [Create](#)

19. It will generate a Subnet id in the next page

Subnets > Create subnet

Create subnet

✓ The following Subnet was created:

Subnet ID [subnet-0bbd5624a8c92f4fc](#)

[Close](#)

20. Select a Subnet and enable the Auto-Assign IP Address for it

Create subnet [Actions](#)

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
Public	subnet-0c9ca43876816e0a0	available	vpc-024052fa68fb95be3 ...	10.0.1.0/24	251	-
Private	subnet-024a8c92f4fc	available	vpc-024052fa68fb95be3 ...	10.0.2.0/26	59	-
	subnet-9d7f7bf5	available	vpc-9d7f7bf5 aws_VPC	172.31.16.0/20	4091	-
	subnet-9d7f7bf5	available	vpc-9d7f7bf5 aws_VPC	172.31.32.0/20	4091	-
	subnet-9d7f7bf5	available	vpc-9d7f7bf5 aws_VPC	172.31.0.0/20	4091	-

Select Modify Auto-Assign IP Address to enable auto-assign

Subnet: subnet-0c9ca43876816e0a0

Description

Subnet ID	subnet-0c9ca43876816e0a0	State	available
VPC	vpc-024052fa68fb95be3 Custom_VPC	IPv4 CIDR	10.0.1.0/24
Available IPv4 Addresses	251	IPv6 CIDR	-
Availability Zone	ap-south-1a (aps1-az1)	Route Table	rtb-08d29780878c649d3
Network ACL	acl-061e7599e0114ae09	Default subnet	No
Auto-assign public IPv4 address	No	Auto-assign IPv6 address	No
Owner	393106192112		

21. On the next page select the check box and save to enable the Auto-Assign IP Address in the description of the Subnet it will be enabled or yes

Subnets > Modify auto-assign IP settings

Modify auto-assign IP settings

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for an instance launched in this subnet. You can override the auto-assign IP settings for an instance at launch time.

Subnet ID subnet-0c9ca43876816e0a0

Auto-assign IPv4 ☒ Enable auto-assign public IPv4 address ⓘ

Click on check box

* Required

Cancel Save

22. By default a Route Table and NACL will be created during the creation of VPC

23. Since we are creating private RT we are using the default RT as public and we need two Route Table

24. On the left select Route Table to open and Select Create Route Table initiate the process

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Create route table Actions

Filter by tags and attributes or search by keyword

1 to 2 of 2

Name	Route Table ID	Explicit subnet association	Main	VPC ID
<input checked="" type="checkbox"/> Public_Route_Table	rtb-08d29780878c649d3	-	Yes	vpc-024052fa68fb95be3 ...
<input type="checkbox"/> AWS_Route_Table	rtb-d430cabf	-	Yes	vpc-9d7f7bf5 aws_VPC

Route Table: rtb-08d29780878c649d3

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

25. Enter the RT name and select the VPC

Route Tables > Create route table

Create route table

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

Name tag Private_Route_table ⓘ

VPC* vpc-024052fa68fb95be3 ⓘ Select the VPC

* Required

Filter by attributes

vpc-9d7f7bf5 aws_VPC


vpc-024052fa68fb95be3 Custom_VPC

Cancel Create

26. Route Table id will be generated

Route Tables > Create route table

Create route table

 The following Route Table was created:

Route Table ID `rtb-09b01c103133d3fe1`

Close

27. Select Public RT to add the public route by click on edit route in the Routes

Create route table Actions ▾

Filter by tags and attributes or search by keyword K < 1 to 3 of 3 > |

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Main	VPC ID
<input checked="" type="checkbox"/>	Public_Route_Table	rtb-08d29780878c649d3	-	Yes	vpc-024052fa68fb95be3 ...
<input type="checkbox"/>	Privatre_Route_table	rtb-09b01c103133d3fe1	-	No	vpc-024052fa68fb95be3 ...
<input type="checkbox"/>	AWS_Route_Table	rtb-d430cabf	-	Yes	vpc-9d7f7bf5 aws_VPC

Route Table: rtb-08d29780878c649d3

Summary **Routes** Subnet Associations Route Propagation Tags

Edit routes Select edit route to make accessible through internet

View All routes ▾

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

28. Enroll the Public access to the route and click on save routes late on it will display Routes successfully edited

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0 Public Access ▾	igw-0f2646868fed174a2 ▾		No

Add route Select Add Route to add a new entry

Egress Only Internet Gateway Instance

Internet Gateway

NAT Gateway

Network Interface

Peering Connection

Transit Gateway

Virtual Private Gateway

igw-0f2646868fed174a2 Custom_IGW

Select the IGW and add the Custom created IGW

* Required

Cancel **Save routes**

29. It is mandatory to attach the Public Subnet to the Public RT

Create route table Actions ▾

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Main	VPC ID
<input checked="" type="checkbox"/>	Public_Route_Table	rtb-08d29780878c649d3	-	Yes	vpc-024052fa68fb95be3 ...
<input type="checkbox"/>	Privatre_Route_table	rtb-09b01c103133d3fe1	-	No	vpc-024052fa68fb95be3 ...
<input type="checkbox"/>	AWS_Route_Table	rtb-d430cabf	-	Yes	vpc-9d7f7bf5 aws_VPC

Route Table: rtb-08d29780878c649d3

Summary Routes **Subnet Associations** Route Propagation Tags

Edit subnet associations Click on Edit to add the Public Subnet

None found

Subnet ID	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations.		

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0bbd5624a8c92f4fc Private_Subnet	10.0.2.0/26	-
subnet-0c9ca43876816e0a0 Public_subnet	10.0.1.0/24	-

30. Adding the Public Subnet

Route Tables > Edit subnet associations

Edit subnet associations

Route table rtb-08d29780878c649d3 (Public_Route_Table)

Associated subnets subnet-0c9ca43876816e0a0

<input type="checkbox"/>	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-0bbd5624a8c92f4fc Private_Subnet	10.0.2.0/26	-	Main
<input checked="" type="checkbox"/>	subnet-0c9ca43876816e0a0 Public_subnet	10.0.1.0/24	-	Main

* Required

Cancel **Save**

31. Select and add Private Subnet on Private RT

Create route table Actions ▾

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Main	VPC ID
<input type="checkbox"/>	Public_Route_Table	rtb-08d29780878c649d3	subnet-0c9ca43876816e0a0	Yes	vpc-024052fa68fb95be3 ...
<input checked="" type="checkbox"/>	Privatre_Route_table	rtb-09b01c103133d3fe1	-	No	vpc-024052fa68fb95be3 ...
<input type="checkbox"/>	AWS_Route_Table	rtb-d430cabf	-	Yes	vpc-9d7f7bf5 aws_VPC

Route Table: rtb-09b01c103133d3fe1

Summary Routes **Subnet Associations** Route Propagation Tags

Edit subnet associations Select edit to add Private Subnet

None found

Subnet ID	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations.		

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

1 to 1 of 1

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0bbd5624a8c92f4fc Private_Subnet	10.0.2.0/26	-

Route Tables > Edit subnet associations

Edit subnet associations

Route table rtb-09b01c103133d3fe1 (Privatre_Route_table)

Associated subnets subnet-0bbd5624a8c92f4fc

Filter by attributes or search by keyword

<input type="checkbox"/>	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/>	subnet-0bbd5624a8c92f4fc Private_Subnet	10.0.2.0/26	-	Main
<input type="checkbox"/>	subnet-0c9ca43876816e0a0 Public_subnet	10.0.1.0/24	-	rtb-08d29780878c649d3

* Required

Cancel **Save**

32. In Security Group it's mandatory to change the Inbound and outbound rules in order for network connection
33. Identify the SG through the VPC ID and edit the Outbound and Inbound rules and add the All Traffic rule and select Save Rules
34. Changing Outbound Rule

Security Groups

Name	Group ID	Group Name	VPC ID	Type	Description
AWS_Security_Group	sg-a3f670cd	default	vpc-9d7f7bf5	EC2-VPC	default VPC security group
Custom_Security_Group	sg-0d84c0292b8709337	default	vpc-024052fa68fb95be3	EC2-VPC	default VPC security group

Security Group: sg-0d84c0292b8709337

Edit rules Select Edit rules to enroll the All Traffic

Type	Protocol	Port Range	Destination	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	:::0	This rule will be enrolled after adding it on the Edit Rules

Security Groups > Edit outbound rules

Edit outbound rules

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Type	Protocol	Port Range	Destination	Description
All traffic	All	All	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
All traffic	All	All	Anywhere 0.0.0.0/0, :::0	e.g. SSH for Admin Desktop

Search all and select "All traffic"

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

* Required

Cancel **Save rules**

35. Changing Inbound Rules

Create security group

Actions

Filter by tags and attributes or search by keyword

1 to 9 of 9

	Name	Group ID	Group Name	VPC ID	Type	Description
<input type="checkbox"/>	AWS_Security_Group	sg-a3f670cd	default	vpc-9d7f7bf5	EC2-VPC	default VPC security group
<input type="checkbox"/>		sg-04aae52b68503434f	launch-wizard-5	vpc-9d7f7bf5	EC2-VPC	launch-wizard-5 created 2019-10-27T1...
<input checked="" type="checkbox"/>	Custom_Security_Group	sg-0d84c0292b8709337	default	vpc-024052fa68fb95be3	EC2-VPC	default VPC security group
<input type="checkbox"/>		sg-0f958f257b113dbaa	launch-wizard-2	vpc-9d7f7bf5	EC2-VPC	launch-wizard-2 created 2019-10-13T1...

Security Group: sg-0d84c0292b8709337

Description

Inbound Rules

Outbound Rules

Tags

Edit rules

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-0d84c0292b8709337	

Security Groups > Edit inbound rules

Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

Type	Protocol	Port Range	Source	Description	
All traffic	All	All	Custom sg-0d84c0292b8709337	e.g. SSH for Admin Desktop	✕
All traffic	All	All	Anywhere 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop	✕

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

* Required

Cancel

Save rules

36. Create an Ec2 Instance in Custom VPC in both Public and Private Subnets from Zone A and Zone B

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm	Public DNS (IPv4)
Public_Instance	i-0f7cc7020598ef1b4	t2.micro	ap-south-1a	running	2/2 checks ...	N...	ec2-13-234-119-19.ap-
Private_Instance	i-0fae33f412b4457ee	t2.micro	ap-south-1b	running	2/2 checks ...	N...	ec2-13-235-74-109.ap-

Instance: i-0f7cc7020598ef1b4 (Public_Instance) Public DNS: ec2-13-234-119-19.ap-south-1.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID	i-0f7cc7020598ef1b4	Public DNS (IPv4)	ec2-13-234-119-19.ap-south-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	13.234.119.19
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-1-72.ap-south-1.compute.internal
Availability zone	ap-south-1a	Private IPs	10.0.1.72
Security groups	default, view inbound rules, view outbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-024052fa68fb95be3 (Custom_VPC)
AMI ID	amzn2-ami-hvm-2.0.20191116.0-x86_64-gp2 (ami-0ce933e2ae91880d3)	Subnet ID	subnet-0c9ca43876816e0a0 (Public_subnet)

37. Zone A Public Instance

```
C:\Users\Suhail>ping 13.234.119.19
Zone A Public Instance
Pinging 13.234.119.19 with 32 bytes of data:
Reply from 13.234.119.19: bytes=32 time=40ms TTL=238
Reply from 13.234.119.19: bytes=32 time=39ms TTL=238
Reply from 13.234.119.19: bytes=32 time=45ms TTL=238
Reply from 13.234.119.19: bytes=32 time=39ms TTL=238

Ping statistics for 13.234.119.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 39ms, Maximum = 45ms, Average = 40ms
```

38. Zone B Private Instance

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm	Public DNS (IPv4)
Public_Instance	i-0f7cc7020598ef1b4	t2.micro	ap-south-1a	running	2/2 checks ...	N...	ec2-13-234-119-19.ap-
Private_Instance	i-0fae33f412b4457ee	t2.micro	ap-south-1b	running	2/2 checks ...	N...	ec2-13-235-74-109.ap-

Instance: **i-0fae33f412b4457ee (Private_Instance)** Public DNS: **ec2-13-235-74-109.ap-south-1.compute.amazonaws.com**

Description | Status Checks | Monitoring | Tags

Instance ID	i-0fae33f412b4457ee	Public DNS (IPv4)	ec2-13-235-74-109.ap-south-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	13.235.74.109
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-2-26.ap-south-1.compute.internal
Availability zone	ap-south-1b	Private IPs	10.0.2.26
Security groups	default. view inbound rules. view outbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-024052fa68fb95be3 (Custom_VPC)
AMI ID	amzn2-ami-hvm-2.0.20191116.0-x86_64-gp2 (ami-0ce933e2ae91880d3)	Subnet ID	subnet-0bbd5624a8c92f4fc (Private_Subnet)

```
C:\Users\Suhail>ping 13.235.74.109
Zone B Private Instance
Pinging 13.235.74.109 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.235.74.109:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Amazon Reference Link:

1. <https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>

Other's Reference Links:

1. https://www.tutorialspoint.com/amazon_web_services/amazon_web_services_virtual_private_cloud.htm
2. <https://www.youtube.com/watch?v=gUesnoDzNr4>