

Canvas Lab - Step: Workflow of setting VPC

Type @ to insert

1: Create VPC only

Check the range of the IPv4 CIDR, for example: 15,000 private IP address available /18 (16,384 IPs)

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

First VPC

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
192.168.0.0/18
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 **Value - optional**

Q Name X Q First VPC X Remove tag

Add tag

You can add 49 more tags

Cancel Create VPC

2: Create public subnet

Check how many public IP address I need, for example 50 → /26 (63 IPs)

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-03fc2f2d14a9100 (First VPC)

Associated VPC CIDRs

IPv4 CIDRs
192.168.0.0/18

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.

First_VPC_Public_Subnet
The name can be up to 255 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. This subnet's IPv4 CIDR must be within this block.

192.168.0.0/18

IPv4 subnet CIDR block
192.168.1.0/26 64 IPs

Tags - optional

Remove

Add new subnet

Cancel Create subnet

3: 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.

First_VPC_Public_Route_Table

VPC

The VPC to use for this route table.

vpc-03fc2ff2d14af9100 (First 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

Q Name

Value - optional

Q First_VPC_Public_Route_Table

Remove

Add new tag

You can add 49 more tags.

Cancel

Create route table

3.1: Add route to route table

Route table → routes tag → edit routes → add route

[VPC](#) > [Route tables](#) > [rtb-0bfb972bdd3c63081](#) > Edit routes

Edit routes

Destination

192.168.0.0/18

Target

local

Status

Active

Propagated

No

Q

local

-

No

Remove

Q 0.0.0.0/0

Internet Gateway

-

No

Remove

Add route

Cancel

Preview

Save changes

3.2: Subnet Associate (edit from without explicit to explicit)

before:

rtb-0bfb972bdd3c63081 / First_VPC_Public_Route_Table

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

Explicit subnet associations (0)

Find subnet association

Edit subnet associations

< 1 > ⚙

Name

Subnet ID

IPv4 CIDR

IPv6 CIDR

No subnet associations
You do not have any subnet associations.

Subnets without explicit associations (1)

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

Find subnet association

Edit subnet associations

< 1 > ⚙

Name

Subnet ID

IPv4 CIDR

IPv6 CIDR

First_VPC_Public_Subnet

subnet-048aba62ef4d5b40f

192.168.1.0/26

-

After:

4: Create Internet Gateway

4.1: attach IGW to VPC

5: Check NACL

check the inbound rules and outbound rules (100, that states that all traffic, all protocols, all port ranges, from any source (0.0.0.0/0) are allowed to enter (inbound) the subnet. The asterisk * indicates that anything else that does not match this rule is denied.)

6: Create SG

6.1: Inbound rule

Done!