4. Managing Virtual Private Cloud (VPC)

VPC is the backbone of the AWS cloud platform. In order to become an AWS Solutions Architect, you must have a better understanding of the AWS VPC and its components. If you are from the networking background, managing VPC might be very easy for you. However, candidates from the developing background should spend a good amount of time to get familiarized with the AWS VPC and its components such as Internet Gateways, NAT Gateways, Routing tables, VPC Peering, Subnets etc. We have covered all these components in details in the separate sections.

VPC is a separate, isolated, private network in the AWS cloud. By default, the instances from one VPC to another VPC cannot communicate to each other. For some reasons, we may need to have multiple VPCs in the AWS cloud. One use case of having multiple VPCs is that suppose we want to keep our development and production instances logically isolate to each other. Here, we will see how to create, manage, and delete VPCs.

Note: The allowed block size for an AWS VPC can vary between /16 to /28 netmask. It means, you cannot create a VPC with netmask as /15 or as /29.

Recommended links:

- Getting started with AWS VPC.
- http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/getting-started-ipv4.html

---

Note: When you sign up for the free tier AWS account, a default VPC is created for your in each region with default settings. You should not use the default VPC for the production servers neither you should delete it. However, you can always use the default VPC for the testing purposes.

Creating VPC in AWS Cloud

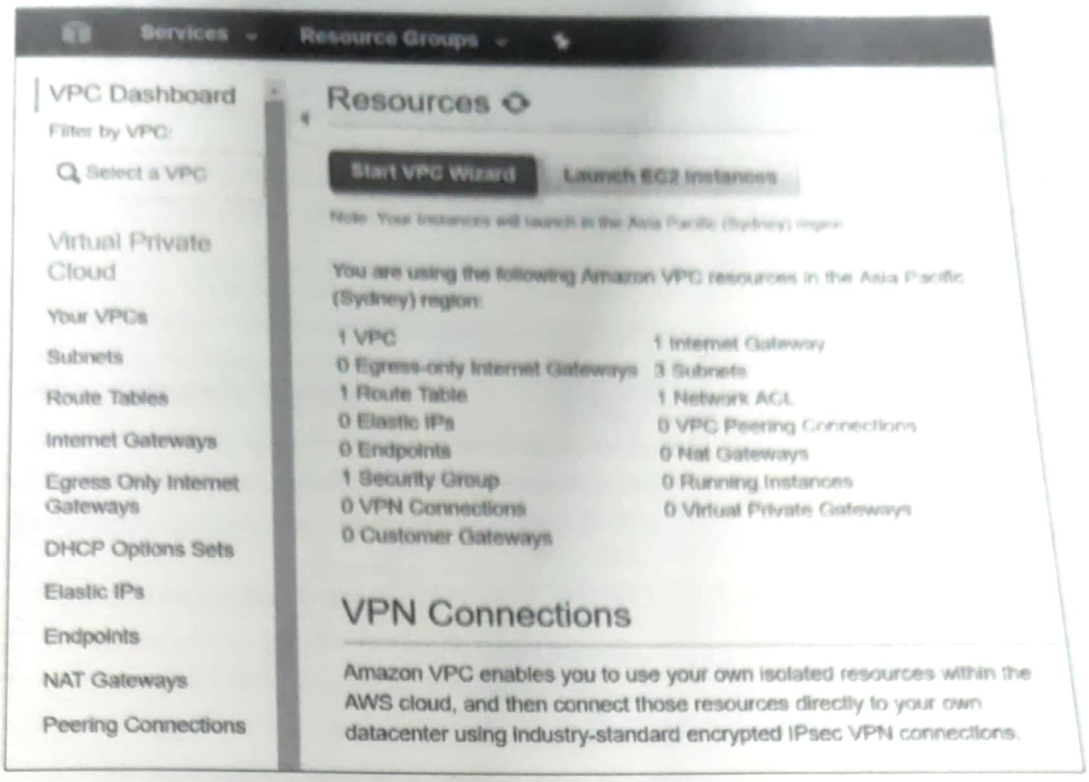
In order to create a VPC, you need to perform the following steps:

1. In the AWS console, search and open the **VPC** dashboard.

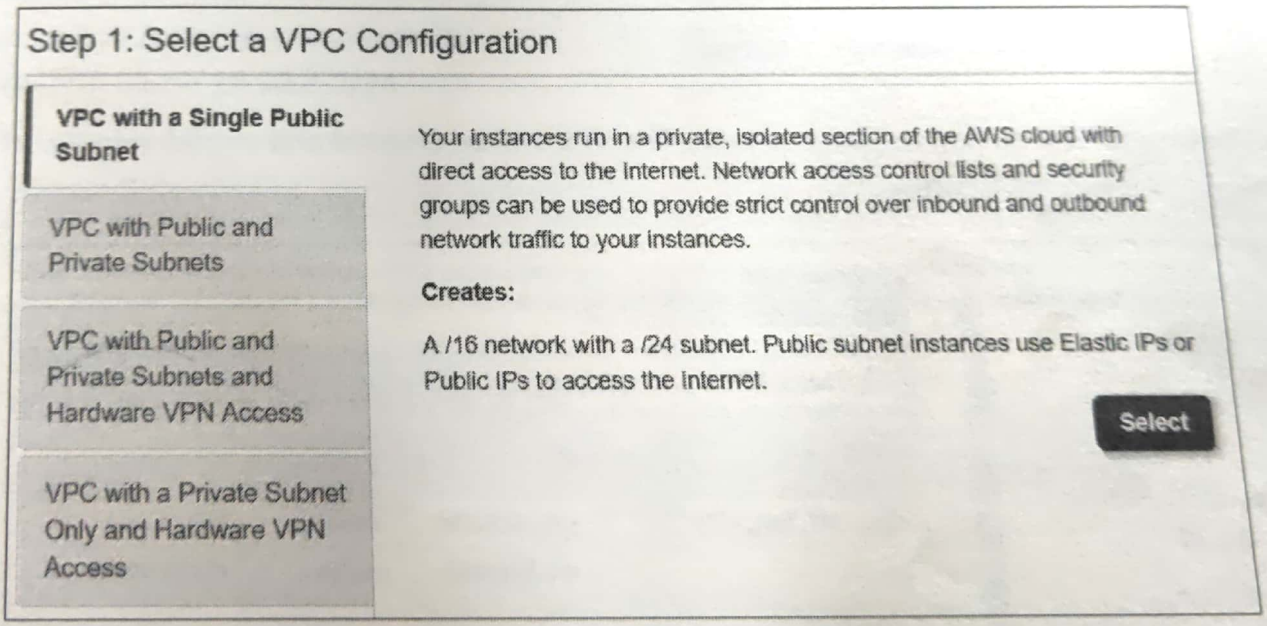
Note: There are two methods to create VPCs: using the Start VPC Wizard and Manual VPC creation. Beginners should use the Start VPC Wizard as it's an easy method to create VPC. Once you become familiar with the VPC components you can directly create and manage VPCs without using the Start VPC Wizard. So, let's get started with the Start VPC Wizard.

---

2. Click the **Start VPC Wizard** option as shown in the following figure.



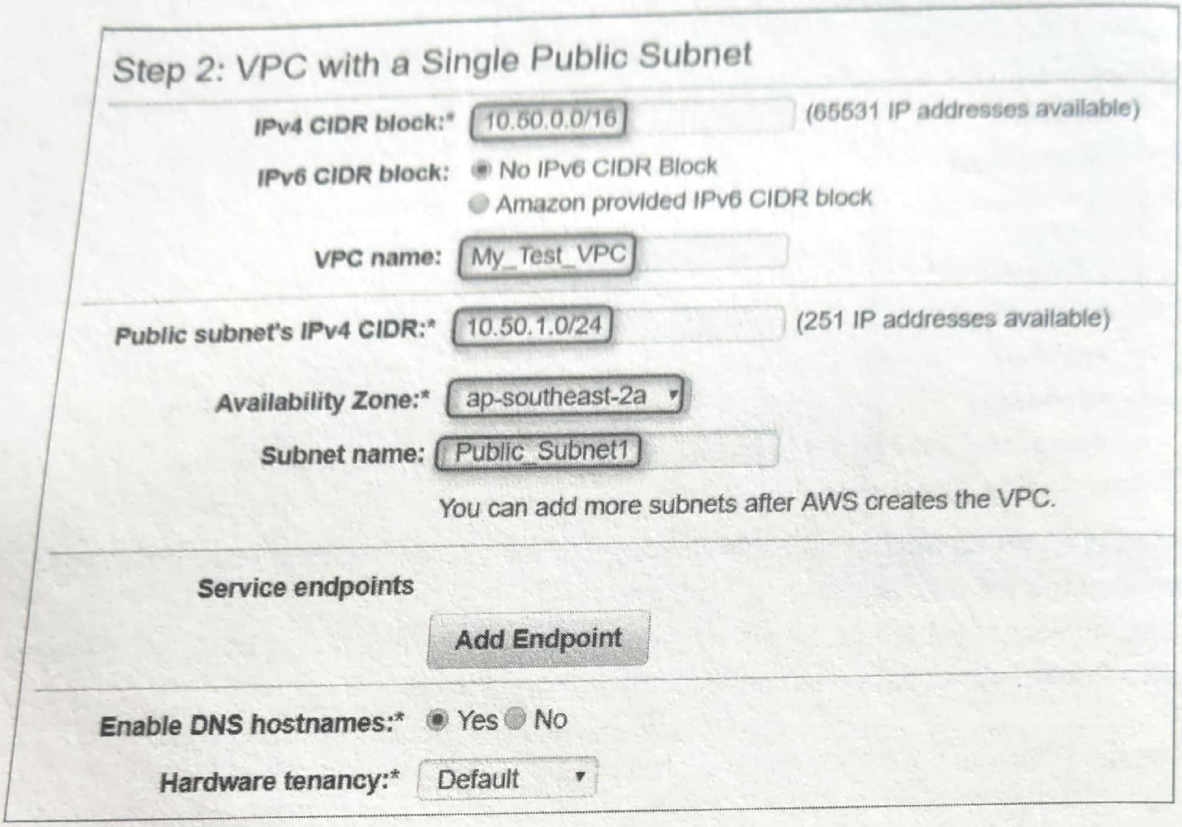
3. On the **Select a VPN Configuration** page, click each of the VPC Configuration options and review the description of the features provided by them.
4. Depending on your requirement, select the appropriate VPC configuration. Here, we will select the VPC with a Public Subnet option as shown in the following figure.



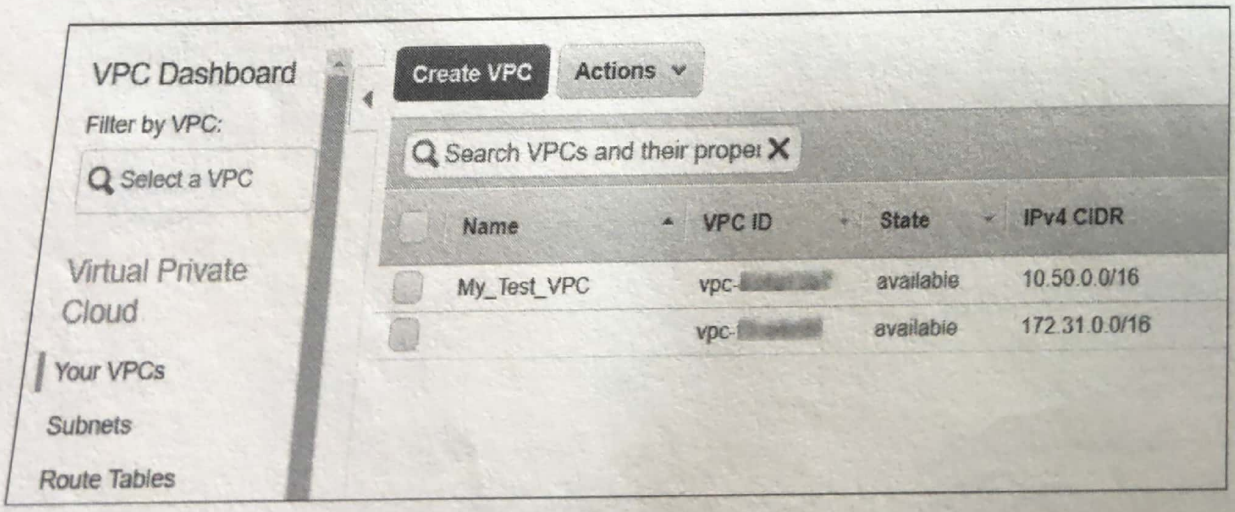
Note: *You can later add more subnets in the VPC and can customize your VPC options as per the requirements.*

---

5. On the next page, specify the VPC name, subnet range, and Availability Zone etc. Here we are going to specify the following values:
   - IPv4 CIDR Block: **10.50.0.0/16**
   - VPC Name: **My_Test_VPC**
   - Public Subnet CIDR: **10.50.1.0/24**
   - Availability Zone: **Select the first availability zone.**
   - Subnet Name: **Public_Subnet1**



6. Click the **Create VPC** button to proceed next. The VPC will be created and available in the VPC list as shown in the following figure.



Creating and Adding Private Subnet in the Existing VPC

ce we had selected the VPC with a Public Subnet option, so we need to create Private subnets arately. A private subnet does not have direct access from the outside AWS network such as the

Internet. All private subnets require a NAT gateway to access the Internet. Typically, backend and database servers should always belong to the private subnets.

If you are interested, you can visit the following link to know more about the AWS VPC and subnets.

- AWS VPC and Subnets Getting Started.
- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

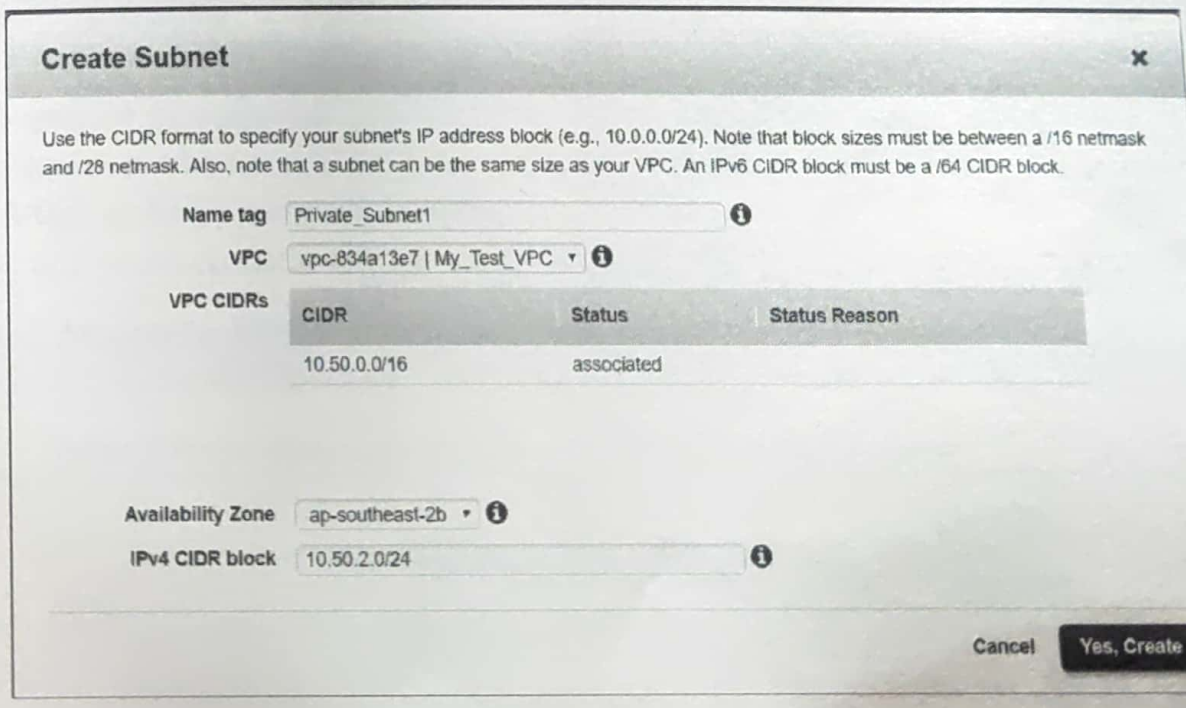
To create a private subnet, you need to perform the following steps:

1. Select the **Subnets** option in the navigation pane and then click **Create Subnet**.
2. On the **Create Subnet** page, specify the following values:
   - **Name tag**: Name of the subnet
   - **VPC**: Select the VPC in which you want to create the subnet
   - **Availability Zone**: Select the zone in which you want to create the subnet
   - **IPv4 CIDR block**: Specify the subnet IP range which must be within the VPC CIDR range.

Note: You cannot specify the IP range for your subnet out of the CIDR range configured for your VPC. For example, if you have configured VPC with the CIDR range as 10.15.0.0/16, then you cannot create a subnet with 10.16.1.0/24 because it violates the IP networking rules.

---

3. For our lab exercise, let's create a Private subnet with the following values:
   - Name tag: **Private_Subnet1**
   - VPC: **My_Test_VPC**
   - Availability Zone: **ap-southeast-2b**
   - IPv4 CIDR block: **10.50.2.0/24**

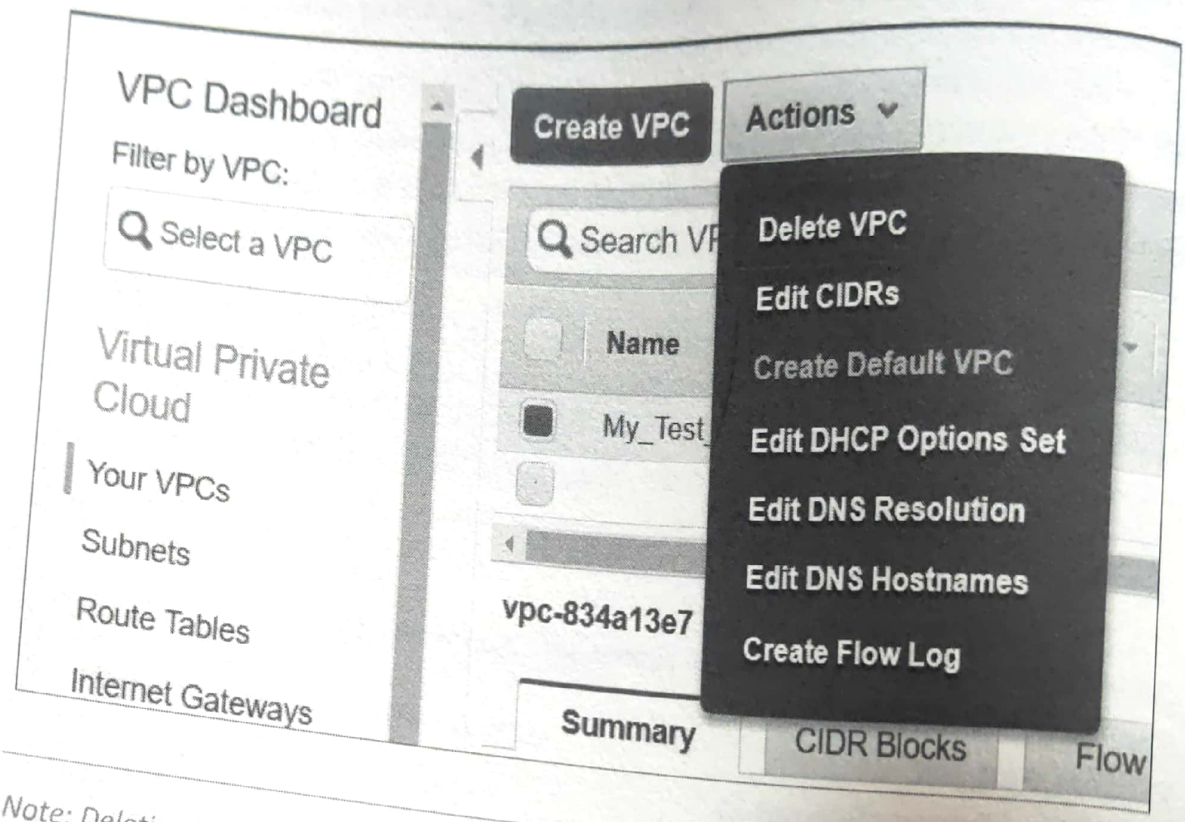


4. Click the **Yes Create** button to proceed. A new private subnet will be added to your existing VPC.

Note: In an upcoming lab, we will also explore how to configure VPC peering between two or more VPCs to allow inter-VPC communication.

Deleting VPC

If you no longer require any VPC for any reason, you can delete it anytime. For this, just select the VPC you want to delete, click **Actions** and then select **Delete VPC** to delete it as shown in the following figure.



Note: Deleting VPC will also delete all its associated components such as Subnets, NAT Gateway, Routing Tables, Internet Gateways, etc. However, if your VPC has EC2 instances (running or stopped), you must first terminate your EC2 instances manually before you could delete the VPC.

Question 03: You can create a VPC with the 192.168.1.0/30 netmask?

A. True

B. False