**1. What is the actual definition of the term “VPC”?**

**Answer:** Well, VPC is a private network space within the Amazon cloud that enables you to launch AWS resources. It’s the actual networking layer of Amazon EC2, about which [we have already discussed](https://www.whizlabs.com/blog/aws-vpc/). Each private network you create on the cloud will be logically separated from other virtual networks in the cloud.

Although the structure of VPC looks similar to a standard network that you’d operate in a data center, a VPC will have the benefits of the scalable infrastructure of AWS. Another major advantage of VPC is that it is fully customizable. You can create subnets, set up root tables, configure network gateways, setup network access control lists, choose IP address range, and many more in a Virtual Private Cloud.

**2. What are the components of Amazon VPC?**

**Answer:** The foremost element in Amazon VPC architecture is VPC network itself. It’s a logically separated part of AWS cloud. It’s possible to define your Virtual Private Cloud’s IP address from the range you’ve chosen. The second element is the Internet Gateway which is the connecting point between your VPC and the public internet. Subnets are the functional parts of your private cloud’s IP address range.

NAT Gateways are used to connect between instances of your private subnet with internet or other AWS services. Customer Gateways are your side of a VPN connection in AWS while Virtual Private Gateways are Amazon VPC side of VPN connection. This type of questions lies under the general or basic AWS VPC interview questions. Whether you are a fresher or have some experience, you may come across such questions so get prepared with the answer.

**Components of Amazon VPC with Brief description:**

|  |  |
| --- | --- |
| **Element** | **Brief description** |
| *Virtual Private Cloud (VPC)* | A logically isolated virtual network in the AWS cloud. You define a VPC’s IP address space from a range you select. |
| *Subnet* | A segment of a VPC’s IP address range where you can place groups of isolated resources. |
| *Internet Gateway* | The Amazon VPC side of a connection to the public Internet. |
| *NAT Gateway* | A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet. |
| *Hardware VPN Connection* | A hardware-based VPN connection between your Amazon VPC and your datacenter, home network, or co-location facility. |
| *Virtual Private Gateway* | The Amazon VPC side of a VPN connection. The Customer gateway is the customer side of a VPN connection. |
| *Peering Connection* | A peering connection enables you to route traffic via private IP addresses between two peered VPCs |
| *VPC Endpoint* | Enables Amazon S3 access from within your VPC without using an Internet gateway or NAT, and allows you to control the access using VPC endpoint policies. |

**3. What are Internet Gateways in VPC?**

**Answer:** An Internet Gateway is highly available, horizontally scaled VPC component. Gateways establish coherent connections between your Amazon VPC network and the internet. There can be only one gateway associated with each VPC. These are the VPC components that provide NAT (Network Address Translation) for instances which have already assigned public IP addresses. In the case of internet routable traffic, such a gateway provides a target in your VPC route tables.

**4. What is a NAT Device?**

**Answer:** A NAT device in your VPC will enable instances in the private subnet to trigger outbound IPv4 traffic to other AWS services/internet while hindering inbound traffic initiated on the internet. Here when traffic goes out to the internet, IP address gets replaced by NAT device’s address and when the response comes back to the instances, the device translates the address of instances back to the private IP addresses. AWS has two types of NAT devices – NAT instance and [NAT gateway](https://www.whizlabs.com/blog/nat-gateway/). Linux AMIs are configured to run as NAT instances. NAT does not support IPv6 as well.

**5. What is a subnet in VPC?**

**Answer:** According to AWS documentation, subnets are nothing but a range of IP addresses in your VPC. It is possible to launch the resources of AWS into your desired subnet. For resources that need internet access, you can use a public subnet. Whereas for resources that don’t need the internet, a private subnet is sufficient.

The default subnet in your VPC must have the netmask value 20 that can give up to 4096 addresses per subnet. The subnet is always confined within a single availability zone whereas VPC can span across multiple zones.

Want to become an AWS Certified Architect? Start your preparation now for the [AWS Certified Solutions Architect Associate](https://www.whizlabs.com/aws-solutions-architect-associate/) exam.

**6. What is the default VPC? Explain its advantages.**

**Answer:** The questions based on default VPC are among the top AWS VPC interview questions. It’s a logically isolated virtual network that gets created automatically in AWS cloud for an account when the user makes use of Amazon EC2 resources for the first time.

You can alter the components of the default VPC as per your need. There are several advantages of a default VPC. Here, a user can access high-level features such as different IPs, network interfaces without creating a separate VPC or launching instances.

**7. What is ELB (Elastic Load Balancing) and how does it affect VPC?**

**Answer:** As the name implies ELB is a load balancer service for AWS deployments. A load balancer divides the amount of work a computer has to do into more computers and get it done faster. In the same way here ELB distributes incoming application traffic into multiple targets like EC2 instances.

There are 3 types of ELBs to ensure scalability, availability, and security for ensuring your applications as fault tolerant. These are **classic, network, and application load balancers**. Network and application load balancers can be used in conjunction with VPC and these can route traffics to targets within VPCs.

**8. What do you know about VPC Peering?**

**Answer:** You may be asked about the AWS VPC peering bandwidth in AWS VPC interview. It’s simply the networking connection between two VPs in the same network. It’s possible to create a VPC peering connection between your own VPs or VPC with another AWS account within the same region. It’s not needed for AWS to break the existing VPC infrastructure to enable VPC peering. There is no need of a special hardware for this purpose. It’s not creating a VPN connection or network gateway within the AWS.

The main intention behind such a connection is to facilitate data transfer across multiple VPNs spanning different AWS accounts. This type of peering is a one-to-one relationship wherein transitive connection is not supported.  And while talking about AWS VPC peering bandwidth, there are no bandwidth limitations for peering connections as well.

**9. What are the differences between Private, Public & Elastic IP Addresses?**

**Answer:** The questions based on [Elastic Network Interfaces](https://www.whizlabs.com/blog/elastic-network-interface/) are among the most common AWS VPC interview questions.

As the name implies, private IP addresses are IP addresses that aren’t accessible over the internet. If you want to communicate between instances in the same network, private IPs are used. At an instance launching time, a private IP from subnet’s IP address range and a DNS hostname is assigned to eth0 of the instance (default network interface).

A private IP address remains associated with the network interface will get released only when the instance is terminated (not when the instance is stopped or restarted). On the contrary, a public IP address is easily accessible over the internet.

When you launch a VPC instance, one public IP will automatically assign to the instance which isn’t associated with your AWS account. Every time you restart and stop the instance, AWS will allocate a new public IP to the instance. The main difference between a public and elastic IP is that elastic IP is persistent. It’ll be associated with your AWS account until you terminate it. Anyhow, you can detach elastic IP from one instance and attach the same IP to a different instance. Elastic IP is also accessible over the internet.

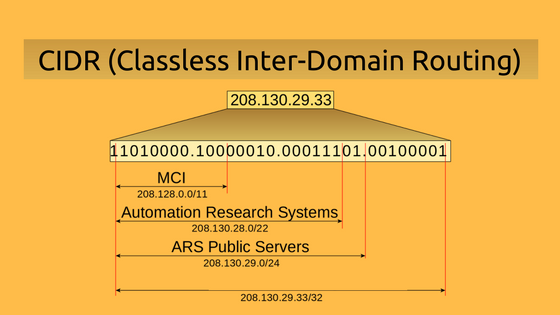
**10. Is there any limit to the number of VPCs, subnets, gateways, VPNs that I can create?**

**Answer:** Yes, there is definitely a limit. You can create **5 VPCs per region**. If you want to increase this limit, you’ve to increase the number of internet gateways by the same number. And, per VPC 200 subnets are allowed. 5 elastic IP addresses are allowed per region. The number of Internet, VPN and NAT gateways per region is also set to 5.

Anyhow, customer gateways are allowed to 50 per region. One can create 50 VPN connections per region. It is highly recommended to cover questions based on connectivity while going through the top AWS VPC interview questions.

**11. Can you illustrate what is CIDR Routing in VPC?**

**Answer:** The questions based on IP address are the common among frequently-asked AWS VPC interview questions. This CIDR question can be answered in the following manner. [Classless inter-domain routing (CIDR)](https://www.whizlabs.com/blog/cidr-classless-inter-domain-routing/) is a set of Internet protocol (IP) standards that are used to allocate IP addresses for networks and individual devices. With CIDR, a single IP address can be used to pick many unique IP addresses.



Generally, A CIDR IP looks like a normal IP address except there is a slash followed by a number in CIDR. This part is called the IP network prefix. In VPC, CIDR block size can be from /16 to /28 in case of IPv4. When you’re creating a VPC, you actually have to specify a range of IP address in form of CIDR just like 10.0.0.0/16. This CIDR is the primary CIDR block of your VPC.

CIDR offers the benefits of effective management of available IP address space and reduce the number of routing table entries. If you are still wondering [what does CIDR stand for](https://www.whizlabs.com/blog/cidr-classless-inter-domain-routing/), learn more!

**12. What are Security Groups in VPC?**

**Answer:** In VPC, a security group’s function is to manage the traffic for the instances. Instances can be single in number or many. Actually, it does act as a virtual firewall that can control inbound and outbound traffic for different EC2 instances. You can manually add rules to each security group to control the traffic within the associated instances.

In AWS console, security groups can be located in both VPC and EC2 sections. By default, all security groups allow outbound traffic. In the same way, you can define rules to allow inbound traffic. But one thing- you are only allowed to create “**allow**” rules rather setting up denial rules to restrict security permissions. Also, it’s possible to change the rules of a security group irrespective of the time and the process of changing rules will take place instantly. You may come across questions on security in an AWS VPC interview, so we’ve included it in our list of the best AWS VPC interview questions.

**13. What do you mean by Network ACLs (Access Control List) in VPC?**

**Answer:** Network ACLs does the similar function of a network security group in VPC; IE controlling inbound and outbound traffic in VPC. The main difference between a network ACL and a security group is that the latter’s role is to act as a firewall for associated EC2 instances whereas an ACL’s role is to serve firewall job for associated subnets. Your VPC generates an ACL automatically by default and it’s modifiable. Unlike a security group, this default network ACL allows all inbound and outbound traffic by default. And it’s possible to associate an ACL with multiple subnets. But at a time, only one subnet can be associated with a network ACL.

*You can also create your own custom ACL and it can be associated with a subnet. Such an ACL denies all types of inbound/outbound traffic until you add rules to it.*

**14. What is stateful and stateless filtering?**

**Answer:** A stateful filtering checks the origin of the request and triggers automatic replay to the originating computer. On the other hand, stateless filtering only examines the source and destination IPs ignoring whether it’s a new request or replay to a request.

In VPC, security groups carry out stateful filtering whereas network ACLs perform stateless filtering. Filtering based questions are generally asked in the interview among other popular AWS VPC interview questions so you need to prepare yourself with the answer.

**15. What are the functions of an Amazon VPC router?**

**Answer:** VPC router allows Amazon EC2 instances within subnets to interact with Amazon EC2 instances in other subnets within the same VPC. Virtual private gateways, subnets and Internet gateways, etc. can also communicate with each other by means of a VPC router.

**16. How much Amazon charge you for sharing their cloud space with you?**

**Answer:** Basically for a VPN connection to your VPC, Amazon charges nearly **$0.5 for an hour**. There is an option to terminate your VPN connection through AWS consoled if you don’t want to charge for this.

AWS internet gateway pricing charges vary through different geographic locations. You’ll be charged from **$0.045 up to $0.054** per gateway-hour and GBs of data processed based on your location. Similarly, in the case of VPC peering pricing, the rates depend on the location of VPCs and peering connection. If both are in the same region, the charge of transferring data within a peering connection remains same as the transfer of data within the zone itself.

In case if they are placed in different regions, region data rate costs will apply. You may come across at least **one question based on VPC peering pricing** so here we’ve covered it under the most common AWS VPC interview questions and answers.

**17. What is PrivateLink from AWS?**

**Answer:** PrivateLink provides utmost availability and scalability for AWS customers to access their services maintaining the traffic within the AWS network. It delivers private connections between VPCs, on-premises applications, etc. securely on Amazon network.

**18. What is ClassicLink in VPC?**

**Answer:** If you want to connect Amazon EC2-classic instances to VPC, you have to use ClassicLink. This work only within the same region and this makes use of private IP addresses. Its working is simple- you just have to enable ClassicLink in your VPC account and associate a security group from VPC to EC2-classic instance.

**19. What is so special about VPC that stands out it from other private clouds?**

**Answer:** There’s no need for a particular hardware, physical data centers or virtual private networks if you want a private network within the cloud – AWS VPC will provide it. The advanced security features of VPC makes it almost invulnerable to privacy & security threats.

### 1. What exactly is AWS VPC?

**Ans:**Cloud computing is based on Virtual Private Cloud ( VPC). This is the basic foundation of the AWS platform. Any of the advanced services of AWS can not be accessed without a VPC network. You will get a logically isolated section dedicated to a virtual network platform. Through this cloud, businesses can access customer details and data in a single window. It provides innovative new business approaches.

|  |
| --- |
|  |

### 2. What are the features available in AWS VPC?

**Ans:**This AWS VPC provides the given below features:

1. IPv4 and IPv6 address book.
2. Internet connectivity.
3. Subnet creation.
4. Route tables.
5. Elastic IP addresses.
6. Network/ Subnet security.
7. Additional networking services.

### 3. Where do VPCs live?

**Ans:**These VPC’s are existing in the AWS roundabout. This AWS around a geographic area. It can be around the world in Amazon's clustered data centers. It is lived in that assigned geographical area only to maintain customer distribution. So that in different areas customers can not set up another VPC in another geographical area.

### 4. Name a few companies that are using AWS VPC?

**Ans:**A few top listed companies are

1. Google (USA)
2. Microsoft (USA)
3. Alibaba (China)
4. AWS (USA)
5. OVH ( France)
6. Huawei ( China)
7. Rackspace ( USA)
8. CenturyLink( USA)
9. DXC ( USA)
10. Atos ( France)

### 5. Tell me the scope of the VPC market?

**Ans:**

**Scopes are:**

1. Agility
2. Security.
3. Easy hybrid cloud deployment.
4. More performance.
5. Customer Satisfaction.
6. More resources in channel innovation.

### 6. Is VPC work globally?

**Ans:**Yes, VPC works globally. All its components are also working globally. Obviously, they are divided into zone to crate Subnet networks.

### 7. Do you think that AWS VPC is equivalent to Azure?

**Ans:**Absolutely not. One virtual network is available in Azure, but they are not the same or related. Both of them have a few common features and different key features also.

### 8. Explain to me why Amazon thought to create VPC?

**Ans:**Amazon has lots of physical data centers throughout the world. Now they were looking forward to creating virtual data centers. These data centers needed virtual networks and virtual network access. To manage this virtual cloud they have created VPC which actually gives access to clients in the virtual network with a private cloud zone. They kept access to other Amazon services.

|  |
| --- |
|  |

### 9. Tell me the basic difference between VPC and VPN?

**Ans:**VPC is from Amazon Web Services. It has been created as per zone for giving access to clients. It depends on multiple Subnet. But a VPN is a gateway, actually. This is the access point of the VPN network.

### 10. How many VPC can be created in AWS Zone?

**Ans:**You can create by default only 5 VPC in a single AWS zone.

## AWS VPC Interview Questions and Answers for Freshers

### 11. How can you connect your dedicated VPC network to the internet?

**Ans:**Yes, we can use AWS VPC to enable our internet gateway. It gives permission to EC2 occurrences in VPC to directly access the internet. There are other options also.

We can also follow the given below steps:

1. By using hardware, virtual private network connection, and corporate data centers.
2. By using the internet through an internet gateway.
3. By using both the internet and corporate data center.
4. By using other VPC peering conditions.
5. By using other AWS.

### 12. What steps need to be followed while setting up VPC?

**Ans:**If we want to build up our custom VPC, please follow the given below steps:

1. First, we need to create a virtual private cloud.
2. After that need to create subnets.
3. Now need to create an internet gateway.
4. Need to attach internet gateway with VPC.
5. Need to create a routing table.
6. Now add that created gateway in the new route table.
7. Do subnet association with the routing table.
8. Need to create a database server for the private subnet and a web server for the public subnet.
9. Need to create a new secured group of NAT.
10. Need to add HTTP and HTTPS inbound rules to allow traffic from private subnet IP.
11. Need to create elastic IP.
12. Tag this elastic IP with NAT.
13. Now deactivate the check for NAT.
14. Need to add this NAT in the base route table initially.

### 13.Tell me about the advantages of AWS VPC?

**Ans:**There are a few advantages, they are:

1. Provide a complete process to build a virtual network.
2. No need for hardware, any physical data center, or VPN.
3. Full power access with control over your network.
4. EC2 instance is available to connect to the internet.
5. Can do enhanced security level in VPC with EC 2 instances.

### 14. Can we monitor the network traffic in VPC?

**Ans:**Yes, we can monitor the network traffic in VPC. There are flow logs that we need to follow.

|  |
| --- |
|  |

### 15. Differentiate between stateful and stateless filtering?

**Ans:**

|  |  |
| --- | --- |
| **Stateful Filtering** | **Stateless Filtering** |
| 1. Request origination point will be tracked. | 1. Request origination point  doesn't matter. |
| 2. Reply will be sent automatically. | 2. Doesn’t matter reply is sent  automatically or not. |
| 3. Reply returns to the originated computer. | 3. Reply returns to the destination  IP address and port. |

### 16. Can we use our existing AMIs in AWS VPC?

**Ans:**Yes, we can use our existing AMIs in the AWS VPC in the same registered zone.

### 17. Is it secure if we run an EC2 instance with AWS VPC?

**Ans:**AWS EC2 instances are very secure for the AWS VPC network. It can control both inbound and outbound traffic in the same zone. Once the EC2 instance declined any traffic, further, that traffic is not allowed.

### 18. Tell me the differences between security groups in VPC and ACLS in VPC?

**Ans:**

|  |  |
| --- | --- |
| **VPC Security group** | **VPC ACLS** |
| 1. Fix the traffic coming from EC2 instances. | 1. Fix the traffic coming from Subnet. |
| 2. It can be used to set only allow. | 2. It can be used to set allow and deny both. |
| 3. Filter traffic between the same instances in the same Subnet. | 3. Doesn’t filter traffic between the same instances  in the same Subnet. |
| 4. Perform stateful filtering. | 4. Perform stateless filtering. |

### 19. How can you find out the available zones for your Subnet?

**Ans:**Always keep remembering that while we are creating a subnet we need to mention the available zone. By using VPC Wizard, we can choose an available zone for the subnet. We can specify the available zone by using the API or CLI. If we don’t mention the available zone, then by default no permission options will be activated. The system will be choosing the available zone.

### 20. Explain default VPC?

**Ans:**Default VPC means, it has been created by the system when one user is accessing first time any EC2 instance. Then one isolated virtual network will be created automatically in the same AWS VPC account.

### 21. Can we know that our configured account will be by default VPC?

**Ans:**Actually, the EC2 instance mentions the launching platform and the assigned zone. It also mentions whether you are a by default VPC or not. We can cross-check the zone in the navigation bar.

### 22. Do we need prior knowledge to use them by default VPC?

**Ans:**The answer is no. We can find out about it from the AWS management console in a by-fault VPC. AWS used to create one by default VPC. We need to create a default subnet for each available zone. Default VPC will be connected to the internet through the gateway automatically.

### 23. Do we use existing AWS EBS snapshots?

**Ans:**Obliviously, we can use existing AWS EBS snapshots if they are from the same VPC zone.

### 24. Tell me how you can boot any AWS EC2 instance from AWS EBS inside AWS VPC?

**Ans:**We need to use AWS EBS inside AWS VPC. The same IP address needs to be started, stopped, and restarted.

### 25. How can you use AWS EC2 reversed instance with AWS VPC?

**Ans:**We can use AWS EC2 reversed instances if we do have purchased instances. AWS doesn’t look at whether we are buying instances run in AWS VPC or Standard AWS EC2. By default, AWS will charge for lower reversed instances, so we need to pay the lowest amount. But it depends upon the AWS VPC specified.

|  |
| --- |
|  |

### 26. Do you think that we can delete the default VPC?

**Ans:**Yes, we can delete it from the AWS console, in that case, if we connect with the AWS support team then they can help us to retrieve the old default VPC.

### 27. By any chance, if we delete one of the peering connections, do you think another peering connection can access the VPC?

**Ans:**No, it can not work. Another peering connection can be stopped anytime. It hampers two-way traffic flows.

### 28. If we have one EC2 instance, can we get one by default VPC?

**Ans:**In this case, we need to try in those zones, where by using this existing EC2 instance no VPC has been created earlier. To support the present platform attributes we need to set EC2 and VPC.

### 29. If somehow one peering connection falls down, then how do we need to manage it?

**Ans:**We can use the existing VPC infrastructure to create a peering connection. Now, this peering connection doesn’t like any VPN gateway. The most important point is, that it doesn’t rely on any hardware. So there is less chance of communication failure.

### 30. Do you think that we can create a peering connection of any VPC in another VPC zone?

**Ans:**I think we can not do this. By default, a peering connection can be done within the same VPC zone.

## AWS VPC Interview Questions and Answers for Experienced

### 31. Can we add more than two network interfaces in one EC2 instance?

**Ans:**Yes, we can add more than two network interfaces in one EC2 instance, but it depends on the EC2 instance type. We need to follow the EC2 instance guidelines.

### 32. Do you think there are any bandwidth limitations for peering connections?

**Ans:**Yes. There are bandwidth limitations for peering connections. The peer VPC bandwidth is equal to instances bandwidth in the same VPC.

### 33. Explain the classic link?

**Ans:**AWS VPC classic link is most important to connect EC2 instance classic form with the VPC using IP address. We need to activate this link in the VPC account. All by default rules will be applicable as per the VPC security group between the EC2 classic instance and the instance in the VPC.

### 34. Explain to me how we use a classic link?

**Ans:**If we want to use a classic link, then we need to activate at least one VPC in our account, particularly for the classic link. Now we need to tag one security group from the VPC with the expected classic link. Now our EC2 classic instance is connected to a VPC. This classic link is now a member of a security group in VPC.  Please remember that the EC2 classic instance can not be connected to more than one VPC at a time.

### 35. Do you think EC2 classic is becoming a member of VPC after connecting?

**Ans:**No, EC2 classic instance can not be a member of VPC. Whereas it becomes a member of the VPC security group with the same instance. It has to follow all sets of rules.

### 36. How can we modify the VPC route table? Is it possible?

**Ans:**Yes, we can modify the VPC route table. This route table is related to the specific subnet and internet gateway.

### 37. Explain to me how the AWS VPC router works?

**Ans:**This AWS VPC router allows the AWS EC2 instance to connect with another EC2 instance from another subnet but from the same VPC. It also allows subnet, internet gateway, and virtual private gateway to communicate with each other. Note that the network usage data is not available from the router.

### 38. How does one hardware VPN connection work with AWS VPC?

**Ans:**One data center can connect hardware VPN with AWS VPC. AWS supports internet protocol security VPN connections only. The encrypted data will be transferred. VPN connection helps in data security while transiting. No internet gateway is required to establish a hardware VPN connection with AWS VPC.

### 39. Is there a VPC for which we can not connect the classic link?

**Ans:**Yes, we can not connect classic links with classes inter-domain routing. That router range will be 10.0.0.0/8, with the exception of 10.0.0.0/16 and 10.1.0.0/16. Even if the VPC route table entry points to 10.0.0.0/8 classless inter-domain routing space to target other than local only.

### 40. How can we connect my VPC to the corporate data center?

**Ans:**If the hardware VPN is connected to the existing network, then AWS VPC allows us to interact with the AWS EC2 instance within the same VPC network.

### 41. How can we assign IP address ranges to VPC?

**Ans:**We need to assign one single classless internet IP address block when we create a VPC. The address will be the subnet within the same VPC. One VPC can assign at most only one IP address. Currently, multiple IP addresses assigning is not allowed in AWS. If we try to create multiple IP addresses by overlapping, then AWS won’t give permission to connect with the same VPC. We are requesting to follow non-overlapping IP address ranges.

### 42. What are the default IP address ranges for a default VPC?

**Ans:**The default range is 172.31.0.0/16.

### 43. What do you think, can we change the VPC size?

**Ans:**Absolutely not. We can not change the VPC size once it’s created. But if required then we need to delete the same VPC from the console and need to create a new one.

### 44. Tell me, how many subnets can we get per VPC?

**Ans:**We can get only 200 subnets per VPC. If we want to create more then we need to contact the AWS support team.

### 45. Please whether any fixed size is applicable for a subnet?

**Ans:**Yes, the minimum size is 14 IP addresses for IPv4. Note down that subnets can not be larger than in size from crated VPC.

### 46. Can we assign one private IP address to one AWS EC2 instance within the same VPC?

**Ans:**Yes, we can do this. Once we are launching the AWS EC2 instance within a VPC, we may specify the primary IP address for that particular instance. Suppose, we forgot to mention the primary private IP address, then AWS will automatically assign an IP address range to the subnet. We can also assign a secondary private IP address at the time of instance launching.

### 47. If the server is not managed by the VPC DNS, what will be the solution?

**Ans:**We need to activate DNS hostname resolution. This will resolve these issues automatically.

### 48. Explain the security group in VPC?

**Ans:**This security group is actually like a virtual firewall for the AWS EC2 instance. It can control inbound and outbound traffic. One can assign 5 security groups to one instance. It works on the instance level always. It doesn’t work at the subnet level. So each instance in a particular subnet in the same VPC can be assigned to a different set of security groups. When we want to use AWS VPC API, then also this security group will work.

### 49. Tell me the advantages of default AWS VPC?

**Ans:**We can be benefited like:

1. We will get advanced networking functionalities.
2. We can change the security group within the same VPC.
3. We can get multiple IP addresses.
4. We can get multiple network interfaces.
5. We can launch instances in the same VPC.
6. Explain the data pipeline in AWS VPC.

It allows users to integrate data speed within multiple AWS services. It also analyzes from a single location. We can use a data pipeline to access the source directly. In this case, the data transfer efficiency level will be increased in AWS VPC.