

By OnlineInterviewQuestions.com

AWS VPC Interview Questions

Amazon has always been a dream company for many. Out of all the job designations, a lot of positions open up for AWS VPC developers and the company lookout for professionals who take up the roles and responsibilities thereby delivering results. The developers, on the other hand, have to go through an interview, which might be challenging.

AWS VPC is a commercial service by Amazon, which shall provide the users with a private virtual cloud by using a technology of OpenStack or HPE Helion Eucalyptus. The users can select their own range of IP addresses for VPC. As far as security is concerned, the [AWS](#) VPC provides two-fold security where it uses a security group for a firewall to keep track of the traffic at the instance level and applies network access control list to control traffic at the subnet level. The service is free of cost but if the user accesses the VPC account through VPN then it might be chargeable. Thus, the endless features and great service makes the AWS VPC platform in demand.

Read Best AWS VPC Interview Questions and Answers

Given below are the top 20+ AWS VPC Interview Questions that can be asked by the interview panel during the interview. All the questions listed here are answered in a manner that explains the concept clearly and is easy to understand:

Q1. [What is AWS VPC ?](#)

AWS VPC better known as Amazon Virtual Private Cloud lets you furnish a logically left out department of the Amazon Web Services. Here you can launch Amazon Web Services Resources in a virtual network that is defined by you. You will have absolute control over your virtual networking environment along with the privilege of choosing your own IP address range, network gateways, the configuration of route tables and the creation of subnets. You can also establish a hardware VPN connection between your corporate data center as well as your VPC and influence the AWS cloud as an extension of your corporate data center.

Q2. [How to connect My VPC to the Internet?](#)

It is good news that **Amazon VPC** enables the creation of an Internet gateway. This allows Amazon EC2 occurrences in the VPC to access the Internet directly. There are numerous connectivity options for my VPC. You can connect your Virtual Private Cloud to the following:

- Your corporate data center with the help of a Hardware Virtual Private Network connection
- The Internet through an internet gateway
- The Internet as well as your corporate data center, together. You can do this by using both, the virtual

- private gateway and the Internet gateway.
- Other VPCs through Virtual Private Cloud Peering condition
- Other Amazon Web Services

Q3. What are the elements of Amazon Virtual Private Cloud?

The Amazon VPC contains various elements:

- VPC- a logically secluded virtual network in the Amazon Web Services cloud. You only need to define a Virtual Private Cloud's IP address space from the range that you select
- Internet Gateway- Internet Gateway is the Amazon VPC's side of a connection to the public internet
- Subnet- Subnet is a part of cloud's IP address space from the range that you select
- NAT Gateway- A highly available and managed NAT service for your resources in a private subnet to use the internet
- Virtual Private Gateway- This is the Amazon VPC's side of a VPN connection
- Customer Gateway- It is the user's side of a VPN connection
- Router- Routers interconnect subnets and the direct traffic between Virtual Private Gateways, Internet Gateways, NAT gateways as well as subnets.

Q4. How to build a custom VPC?

In order to build a custom VPC, the following steps must be followed:

- Create a Virtual Private Cloud
- Then create Subnets
- Further create an Internet Gateway
- Attach this new Gateway to your VPC
- Create a new Route Table
- Add the gateway as a route to the new route table
- Add a subnet to the route table's subnet association
- Create a web server for public subnet and a database server for the private subnet
- Create a new security group for the NAT
- Add HTTP and HTTPS inbound rules that let in traffic from the private subnets IP
- Create a NAT for public subnet
- Create an elastic IP
- Associate this IP to the NAT
- Disable destination/source checks for the NAT
- Add NAT to the initial VPC route table as a route.

Q5. What are the advantages of using Amazon Web Services VPC?

It helps you to build a virtual network in the Amazon Web Services cloud. Also, for this process, no hardware, physical data centers or even VPNs will be required. You have absolute power over your own network space. You can control how your network and Amazon EC2 that resources inside your network is actually exposed to the Internet. You also have the leverage to hugely enhance the security options in Amazon VPC to provide more granular access to and from the Amazon EC2 instances in your virtual network.

Q6. Can the network traffic in your VPC be monitored?

Yes, you can use the Amazon VPC flow logs feature to monitor the traffic of network in your Virtual Private Cloud.

Q7. Within which Amazon EC2 Region is Amazon VPC available?

It is available in multiple availability zones in all Amazon EC2 regions.

Q8. Can a VPC span multiple availability zones?

Yes, a virtual private cloud can easily span multiple availability zones.

Q9. How can you differentiate between stateful and stateless filtering?

In case of stateful filtering, the point of origination of request is tracked and the reply is sent automatically to the request, which is then returned to the computer from where it originated.
In case of Stateless Filtering, it doesn't matter whether a new request is generated or an automatic reply is sent to a request, the filter only seeks the origin or destination IP address & port.

Q10. How do you specify which availability zone my Amazon EC2 instances are launched in?

When Amazon EC2 instance is launched you must specify the subnet in which to launch the instance. This instance will be then launched in the availability zone that is associated with the given subnet.

Q11. Can you use your present AMIs in Amazon VPC?

You can very well use your existing AMIs in **Amazon VPC** that is registered within the same region as your VPC.

Q12. Are there any bandwidth limitations for Internet gateways?

An Internet gateway is horizontally scaled, highly available as well as redundant. Thus, there are no bandwidth limitations for Internet gateways.

Q13. How do you secure Amazon EC2 instances running within My VPC?

Amazon EC2 security groups are helpful to secure instances within an Amazon VPC. Security groups in VPC help you to specify both inbound as well as outbound network traffic that is allowed to and from each Amazon EC2 instance. The traffic that is not explicitly allowed to or from an instance is automatically denied.

Q14. What are the differences between security groups in a VPC and network ACLs in a VPC?

Security groups in a VPC mention which traffic is allowed to or from an Amazon EC2 instance. Network ACLs operate at the subnet level and evaluate the traffic that is entering and exiting a subnet. Network ACLs can be used to set both Allow as well as Deny rules. Network ACLs do not filter traffic between the instances in the same subnet. Besides this, the network ACLs performs stateless filtering while security groups perform filtering.

Q15. How do you determine which availability zone my subnets are located in?

When you create a subnet you need to mention the Availability Zone where to place the subnet. When using the VPC Wizard, you can select the subnet's Availability Zone in the wizard confirmation screen. While using the API or the CLI you can mention the Availability Zone for the subnet just as you create the subnet. If you do not specify an Availability Zone, the default "No Preference" option will be selected and the subnet will be created in an available Availability Zone in that region.

Q16. What do you understand by default VPC?

When a user avails Amazon EC2 resources for the first time, a logically isolated virtual network is created automatically in the AWS cloud for the AWS account. In a case where an instance is launched without a subnet ID, it shall automatically be launched in the default VPC.

Q17. State the advantage of a default VPC?

There are several advantages of default VPC. Firstly, if a resource is launched in default VPC, the user can avail the high-end network functions of Amazon VPC along with ease to use Amazon EC2. Secondly, without creating a VPC or launching the instances, the user can still avail several features such as different IP address, altering the security group membership, egress filtering of the security group and several network interfaces.

Q18. Which account is enabled for default VPC?

If a user's AWS account has been created after March then it can launch default VPC resources. If an account has been created before March then it shall use any default VPC in any region specific to that. The region should not have a previous launch or any provision related to Amazon RDS, Amazon Redshift resources etc.

Q19. How will you differentiate between VPC security groups and VPC network ACLs?

When we talk about the VPC security group, it is responsible for tracking only the allowed traffic in EC2 instance, which comes in and goes out from Amazon. VPC network ACLs is a lot different. They are responsible for tracking the traffic only at the subnet level i.e. the traffic coming in or going out of subnet. Network ACLs are unable to filter the traffic in the subnet between instances but can do stateless filtering and are used to set Allow and Deny rules. The security group on the other end can carry out stateful filtering.

Q20. How will you locate the availability Zone of subnets?

In order to create and place the subnet you must be specific about the availability zone. The user can use a VPC wizard for selecting the availability for a subnet with the help of a wizard confirmation screen. The subnet can be created in a specific availability zone with the help of API or CLI. In case the user does not select a specific availability zone then automatically the default zone “No Preference” gets selected. The subnet, therefore, will get created in the zone that’s available in the region.

Q21. What IP addresses range can be used in a VPC?

You can use any **IPv4 address range**, including **RFC 1918** or publicly routable IP ranges, for the primary CIDR block IP addresses range in a VPC.

Q22. what IP addresses range can be used in a VPC?

You can use any IPv4 address range, including RFC 1918 or publicly routable IP ranges, for the primary CIDR block. For the secondary CIDR blocks, certain restrictions apply. Publicly routable IP blocks are only reachable via the Virtual Private Gateway and cannot be accessed over the Internet through the Internet gateway. AWS does not advertise customer-owned IP address blocks to the Internet. You can allocate an Amazon-provided IPv6 CIDR block to a VPC by calling the relevant API or via the AWS Management Console.

Please Visit OnlineInterviewquestions.com to download more pdfs