AWS interview Questions

11 August 2023 11:23

1. You have been assigned to design a VPC architecture for a 2-tier application . The application needs to be highly available and scalable . How would you design the VPC architecture ?

   Answer:
   In this scenario , I would design a VPC architecture in the following way . I would create 2 subnets :public and private . The public subnet would contain the load balancers and be accessible from the internet . The private subnet would host the application servers .

   I would distribute the subnets across multiple Availability zones for High availability Zones for high availability . Additionally , I would configure auto scaling groups for the application servers .

2 . Your organization has a VPC with multiple subnets . You want to restrict a outbound internet access for resources in one subnet , but allow outbound internet access for resources in another subnet . How would you achieve this ?

Answer:

To restrict outbound internet access for resources in one subnet , we can modify the route table associated with that the subnet . In the route table , we can remove the default route (0.0.0.0/0) that points to an internet gate way .

This would prevent resources in that subnet from accessing the internet . For the subnet where outbound internet access is required , we can keep the default route pointing to the internet gateway .

3. You Have a VPC with a public subnet and a private subnet . Instances in the private subnet need to access the internet for software updates . How would you allow internet access for instances in the private subnets ?
   Answer:
   To allow internet access for instances in the private subnet , we can use the Internet Gateway or a NAT instance .

   We would place the NAT Gateway/instance in the public subnet and configure the private subnet route table to send outbound traffic to the Nat Gateway\instance .
   This way , instances in the private subnet can access the internet through the NAR Gateway\instance .

4. You Have launched EC2 instances in your VPC , and you want them to communicate with each other using private IP addresses . What steps would take to Enable this communication ?

Answer:

By default , instances within the same VPC can communicate with each other using private IP addresses .

To ensure this communication , we need to make sure that the instances are launched in the same VPC and are placed in the same subnet or subnets that are connected through a peering connection or a VPC peering link .

Additionally , we should check the security groups associated with the instances to ensure that the necessary inbound and outbound rules are configures to allow communication between them .

5. You want to implement strict network access control for your VPC resources . How would you achieve this ?

   Answer:

   To implement granular network access control for VPC resources , we can use Network Access control lists (ACLS) .

   NACLS are stateless and operate at the subnet level . We can define inbound and outbound rules in the NACLs to allow or deny traffic based on source and destination IP addresses , ports , and protocols .

   By carefully configuring NACLs rules , we can enforce fine-grained access control for traffic entering and leaving the subnets .

6. Your organization requires an isolated environment within the VPC for running sensitive workloads . How would you set up this isolated environment ?

   Answer:

   To set up an isolated environment within the VPC , we can create a subnet with no internet gateway attached .

   This subnet known as isolated subnet will not have direct internet connectivity . We can place the sensitive workloads in this subnet , ensuring that they are protected from inbound and outbound internet traffic .

However , if these workloads require outbound internet access , we can set up a Nat Gateway or Nat instance in a different subnet and configure the isolated subnets 's route table to send outbound traffic through the NAT Gateway/instance .

7. Your application needs to access AWS services , such as S3 securely within your VPC . How would you achieve this ?

   Answer: