Virtual Private Cloud (VPC)

01 March 2025 20:24

1. What is AWS VPC?

AWS **VPC (Virtual Private Cloud)** is a logically isolated network in AWS where you can launch AWS resources, such as EC2 instances, RDS databases, and Lambda functions. It allows you to control networking aspects like IP addressing, subnets, route tables, security groups, and internet access.

2. What are the key components of a VPC?

The main components of a VPC are:

- **CIDR Block:** Defines the IP range of the VPC.
- **Subnets:** Divides the VPC into smaller networks (public & private).
- **Internet Gateway (IGW):** Allows public subnet instances to access the internet.
- **NAT Gateway:** Enables private subnet instances to access the internet securely.
- **Route Tables:** Controls traffic routing within the VPC.
- **Security Groups & Network ACLs:** Manage inbound and outbound traffic.
- **VPC Peering & VPN:** Connects VPCs and on-premises networks.

3. What is the difference between Public and Private Subnets?

Public subnets have direct internet access via an Internet Gateway, while private subnets do not. Instances in private subnets need a NAT Gateway for outbound internet access. Public subnets are used for web servers and load balancers, while private subnets are used for databases and internal applications.

4. How does an Internet Gateway (IGW) work?

An **IGW** allows instances in a public subnet to communicate with the internet.

Steps to enable internet access:

1. Attach an **Internet Gateway (IGW)** to your VPC.
2. Create a **Route Table** and add a route (0.0.0.0/0 → IGW).
3. Associate the route table with the **Public Subnet**.
4. Assign a **Public IP** or **Elastic IP** to instances.

5. What is the purpose of a NAT Gateway?

A **NAT Gateway** allows instances in a **private subnet** to access the internet (for updates, patches, etc.) while preventing inbound internet traffic.

Example Use Case: A private EC2 instance that needs to download software updates but shouldn't be exposed to the internet.

6. What is the difference between Security Groups and Network ACLs?

Security Groups work at the instance level and are stateful, meaning responses to requests are automatically allowed. Network ACLs operate at the subnet level and are stateless, meaning both inbound and outbound rules need to be explicitly defined. Security Groups only have allow rules, while Network ACLs can have allow and deny rules.

7. How does AWS VPC Peering work?

VPC Peering allows **private communication** between two VPCs. It is useful when you need to connect applications in different VPCs **without using the internet**.

◇ **Limitations:**

- VPC Peering does not support transitive peering (A → B and B → C does not mean A → C).
- VPCs must have **non-overlapping CIDR blocks**.

8. What is a VPC Endpoint?

A **VPC Endpoint** enables private connections to AWS services like S3 and DynamoDB without using the public internet.

Types:

1. **Interface Endpoint** → Uses ENI (Elastic Network Interface) for private connections.
2. **Gateway Endpoint** → Uses a route table to route traffic to AWS services (e.g., S3, DynamoDB).

9. What is the difference between VPC Peering and Transit Gateway?

VPC Peering is a one-to-one connection between two VPCs, while AWS Transit Gateway allows multiple VPCs and on-premises networks to interconnect in a scalable manner. Transit Gateway is more suitable for large-scale architectures

10. How do you ensure high availability in VPC?

To achieve **high availability** in VPC:

✔ Use **multiple Availability Zones (AZs)** for redundancy.
✔ Distribute workloads across multiple **subnets**.
✔ Use **Elastic Load Balancers (ELB)** for traffic distribution.
✔ Implement **Auto Scaling Groups (ASG)** for scaling.
✔ Use **Route 53** for DNS-based failover.

11. How do you troubleshoot VPC connectivity issues?

1️⃣ **Check Route Tables** – Ensure correct routing rules.
2️⃣ **Verify Security Groups** – Ensure required inbound & outbound rules are set.
3️⃣ **Check Network ACLs** – Ensure traffic is allowed in ACL rules.
4️⃣ **Confirm Internet Gateway (IGW)** – Ensure it's attached and routes exist.
5️⃣ **Check NAT Gateway** – Ensure private instances route traffic via NAT.
6️⃣ **Use VPC Flow Logs** – Monitor traffic for debugging issues.

12. Can you modify a VPC's CIDR block after creation?

Yes! AWS now allows you to **expand** the CIDR block of a VPC **after creation** but **you cannot shrink it**.

13. What is the difference between an Elastic IP (EIP) and a Public IP?

An Elastic IP is a static IP address that can be reassigned to different instances, while a Public IP is dynamically assigned and changes when an instance is stopped and restarted.

14. What is AWS Direct Connect?

AWS **Direct Connect** provides a dedicated **private** connection from an on-premise data center to AWS VPC. It offers **low latency and high bandwidth**, useful for enterprises requiring secure communication.

15. What is an Elastic Load Balancer (ELB), and how does it work in VPC?

An **Elastic Load Balancer (ELB)** distributes traffic across multiple EC2 instances in a VPC.

Types:

1. **Application Load Balancer (ALB)** → Layer 7, routes based on HTTP/HTTPS.
2. **Network Load Balancer (NLB)** → Layer 4, handles millions of requests with low latency.
3. **Classic Load Balancer (CLB)** → Legacy, combines Layer 4 & Layer 7.