AWS VPC Concepts Explained Simply

What I Learned Today

Today, I learned about key AWS VPC concepts including CIDR ranges, subnets, route tables, Internet Gateway, and NAT Gateway. I now understand how to design a VPC that connects securely and efficiently to the internet.

CIDR and Subnets

CIDR (Classless Inter-Domain Routing) is used to define IP ranges in a VPC.

Example: 10.0.0.0/16 allows for 65,536 IPs.

Subnets break this range into smaller networks, e.g., 10.0.1.0/24.

Main Route Table

The main route table controls how traffic is routed in your VPC. Every subnet is associated with a route table.

For example, to allow internet access, you can route 0.0.0.0/0 to an Internet Gateway or a NAT Gateway.

Internet Gateway

An Internet Gateway (IGW) connects your VPC to the internet. It allows inbound and outbound traffic for instances in public subnets.

Use case: Web servers that need to be accessed from the internet.

NAT Gateway

A NAT Gateway allows instances in private subnets to access the internet, but it blocks inbound traffic. It must be placed in a public subnet.

Use case: Backend servers or databases that need internet access for updates.

Summary: IGW vs NAT

Internet Gateway:

AWS VPC Concepts Explained Simply

- Attached to VPC

- Used for public subnets

- Allows inbound and outbound traffic

NAT Gateway:

- In public subnet

- Used for private subnets

- Allows only outbound traffic

Conclusion

I applied all this information by configuring a VPC in AWS with both public and private subnets, attaching an Internet Gateway and NAT Gateway, and updating route tables accordingly. This was a solid step in deepening my AWS networking knowledge!