Terraform

Terraform: AWS VPC Introduction II

Terraform : Deployment Automation

- **Subnet in VPC -**
- Virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud.
- When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a **Classless Inter-Domain Routing (CIDR) block.**
- **10.0.0.0/16** is the primary CIDR block for your VPC.
- VPC spans all of the Availability Zones in the Region. After creating a VPC, you can add one or more subnets in each Availability Zone.

- **Subnet in VPC -**
- If a subnet's traffic is routed to an internet gateway, the subnet is known as a ***public subnet***.
- If a subnet doesn't have a route to the internet gateway, the subnet is known as a ***private subnet***.
- VPC and subnet sizing for IPv4 -
- **10.0.0.0 - 10.255.255.255 (10/8 prefix)** - User VPC must be /16 or smaller, for example, `10.0.0.0/16`.
- `172.16.0.0` - `172.31.255.255` **(172.16/12 prefix)** - User VPC must be /16 or smaller, for example, `172.31.0.0/16`.
- `192.168.0.0` - `192.168.255.255` **(192.168/16 prefix)** - User VPC can be smaller, for example `192.168.0.0/20`.

Terraform : Deployment Automation

- **Subnet in VPC - To add a CIDR block to your VPC, the following rules apply:**
- The allowed block size is between a **/28** netmask and **/16** netmask.
- CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
- User cannot increase or decrease the size of an existing CIDR block.

Terraform : Deployment Automation

- **Security Group in AWS -**
- ***Security group*** acts as a virtual firewall for your instance to control inbound and outbound traffic.
- Upto 5 SGs can be assigned to Instance in AWS.
- SGs are Instance Level not Subnet Level.

Terraform : Deployment Automation

- **Basics of Security Group in AWS -**
- User can specify allow rules, but not deny rules.
- User can specify separate rules for inbound and outbound traffic.
- Security group rules enable you to filter traffic based on protocols and port numbers.
- By default, a Security Group don’t have any Inbound Rule.
- By default, a security group includes an outbound rule that allows all outbound traffic.
- There are quotas on the number of security groups that you can create per VPC, the number of rules that you can add to each security group, and the number of security groups that you can associate with a network interface.

Will see you in Next Lecture…

See you in next lecture …