TNGS Learning Solutions AWS Solutions Architect Online Course

Virtual Private Cloud (VPC)

Virtual Private Cloud (VPC)

- A Virtual Private Cloud (VPC) is a virtual network that allows you to create isolated and logically segmented sections of the AWS cloud where you can run your resources.
- VPCs offer a high degree of control over your network configuration, including IP address ranges, subnets, route tables, and security settings.

Virtual Private Cloud (VPC)

- **Isolation and Segmentation**: VPCs provide logical isolation, meaning you can create multiple VPCs within an AWS region, and they are isolated from each other. This isolation allows you to run different applications, services, or workloads independently, and it enhances security and privacy.
- **IP Addressing**: You can define your IP address range for your VPC, known as the VPC's IP address space. Within this range, you can create subnets, each with its own IP address range. This allows you to segment your network further and control traffic flow.

Virtual Private Cloud (VPC)

- **Subnets**: Subnets are divisions within a VPC that allow you to organize and isolate resources. You can associate subnets with Availability Zones (AZs) to ensure high availability and fault tolerance. Public subnets typically have routes to the internet, while private subnets do not.
- **Route Tables**: Each subnet is associated with a route table that controls the routing of traffic within the VPC. You can create custom route tables to define how traffic should be routed, allowing you to create network architectures that suit your needs.

Virtual Private Cloud (VPC)

- **Security Groups**: Security Groups act as virtual firewalls for your EC2 instances within a VPC. You can specify inbound and outbound traffic rules to control the traffic that is allowed to and from your instances.
- **Network Access Control Lists (NACLs)**: NACLs are stateless firewalls that control traffic at the subnet level. They are more coarse-grained than security groups and can be used to set broad rules for controlling inbound and outbound traffic.

Virtual Private Cloud (VPC)

- **Internet Gateway (IGW)**: An Internet Gateway is a horizontally scaled, redundant, and highly available component that allows your VPC resources to connect to the internet. It enables instances in public subnets to communicate with the internet and vice versa.
- **NAT Gateway/NAT Instance**: Network Address Translation (NAT) gateways or NAT instances allow resources in private subnets to initiate outbound connections to the internet while preventing inbound traffic from reaching them. This is commonly used for instances that require internet access but should not be directly accessible from the internet.

Virtual Private Cloud (VPC)

- **Peering**: VPC peering allows you to establish private connectivity between VPCs in the same or different AWS regions. This enables resources in one VPC to communicate with resources in another VPC as if they were on the same network.
- **Transit Gateway**: Transit Gateway is a service that simplifies network connectivity between multiple VPCs, on-premises data centers, and remote networks. It acts as a hub for routing traffic between connected networks.

Virtual Private Cloud (VPC)

- **VPC Endpoints**: VPC endpoints allow your VPC to connect to AWS services (e.g., S3, DynamoDB) without traversing the public internet. This enhances security and can improve data transfer performance.
- **VPC Flow Logs**: Flow Logs capture information about IP traffic going to and from network interfaces in your VPC. This data can be useful for monitoring, troubleshooting, and security analysis.

Virtual Private Cloud (VPC)

- AWS VPCs provide the foundational networking infrastructure for your AWS resources and allow you to design secure, scalable, and highly available architectures in the cloud.
- Properly configuring and managing your VPC is essential for building robust and secure AWS environments.