TNGS Learning Solutions
AWS Solutions Architect
Online Course
VPC Peering

VPC Peering

- VPC peering is a networking feature provided by Amazon Web Services (AWS) that allows you to connect two Virtual Private Clouds (VPCs) together, enabling them to communicate as if they were on the same network.
- VPC peering is a private and direct connection that does not involve the public internet.
- It is a powerful feature that facilitates resource sharing, application deployments, and collaboration between different VPCs.

VPC Peering

- **VPC Relationship**: In VPC peering, there are two VPCs involved: the requesting VPC (the initiator) and the accepting VPC (the recipient). The two VPCs can belong to the same AWS account or different AWS accounts, as long as the accounts are in the same AWS region.
- **Private Connectivity**: VPC peering establishes a private, fully-routed connection between the VPCs. It allows instances in one VPC to communicate with instances in the other VPC using private IP addresses as if they were on the same network.

VPC Peering

- **Transitive Routing**: VPC peering is not transitive, meaning that if VPC A is peered with VPC B and VPC B is peered with VPC C, VPC A and VPC C do not have a direct peering relationship. To enable communication between VPC A and VPC C, a separate peering connection must be established.
- **Security Groups and Network ACLs**: When using VPC peering, you can configure security groups and network ACLs to control inbound and outbound traffic between the peered VPCs, just like you would within a single VPC.

VPC Peering

- **Routing**: By default, VPC peering connections use the default route table of each VPC. You can customize the route tables to control how traffic is routed between the peered VPCs. Typically, you add a route entry for the peered VPC's CIDR block.
- **Overlapping IP Addresses**: VPCs with overlapping IP address ranges cannot be peered. Ensure that the IP address ranges of the peered VPCs do not conflict.

VPC Peering

- **DNS Resolution**: You can enable DNS resolution between peered VPCs, allowing instances in one VPC to resolve the private DNS names of instances in the other VPC.
- **AWS Transit Gateway**: For more complex network architectures involving multiple VPCs, AWS Transit Gateway is a scalable and highly available option that simplifies VPC peering by acting as a central hub for connecting multiple VPCs and on-premises networks.

VPC Peering

- **Inter-Region Peering**: VPC peering is typically limited to VPCs within the same AWS region. To establish peering connections between VPCs in different AWS regions, you may use AWS Transit Gateway or other network solutions.
- **Data Transfer Costs**: Data transferred between peered VPCs is typically not charged for data transfer fees within the same AWS region. However, data transfer fees may apply if you're peering VPCs across different AWS regions or to on-premises networks.

VPC Peering

- VPC peering is a valuable tool for building multi-tier applications, enabling resource sharing, and creating a more segmented and modular network architecture within your AWS infrastructure.
- It allows you to connect VPCs while maintaining security and control over traffic flow between them.