www

Assignment Documentation on AWS Transit Gateway

Dated 15-12-2022

By - Ritesh

**Transit Gateway**

A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks. As your cloud infrastructure expands globally, inter-Region peering connects transit gateways together using the AWS Global Infrastructure.

* AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub.
* This connection simplifies your network and puts an end to complex peering relationships.
* Transit Gateway acts as a highly scalable cloud router—each new connection is made only once.
* AWS Transit Gateway helps you design and implement networks at scale by acting as a cloud router.
* As your network grows, the complexity of managing incremental connections can slow you down.
* AWS Transit Gateway connects VPCs and on-premises networks through a central hub.

**Transit Gateway Concepts**

* **Attachments** — You can attach the following:
  + One or more VPCs
  + An AWS Direct Connect gateway
  + A peering connection with another transit gateway
  + A VPN connection to a transit gateway
* **Transit gateway route table** — A transit gateway has a default route table and can optionally have additional route tables. A route table includes dynamic and static routes that decide the next hop based on the destination IP address of the packet. The target of these routes could be any transit gateway attachment. By default, transit gateway attachments are associated with the default transit gateway route table.
* **Associations** — Each attachment is associated with exactly one route table. Each route table can be associated with zero to many attachments.
* **Route propagation** — A VPC, VPN connection, or Direct Connect gateway can dynamically propagate routes to a transit gateway route table. With a Connect attachment, the routes are propagated to a transit gateway route table by default. With a VPC, you must create static routes to send traffic to the transit gateway. With a VPN connection or a Direct Connect gateway, routes are propagated from the transit gateway to your on-premises router using Border Gateway Protocol (BGP). With a peering attachment, you must create a static route in the transit gateway route table to point to the peering attachment.

**Transit gateways working**

You can create, access, and manage your transit gateways using any of the following interfaces:

* **AWS Management Console** — Provides a web interface that you can use to access your transit gateways.
* **AWS Command Line Interface (AWS CLI)** — Provides commands for a broad set of AWS services, including Amazon VPC, and is supported on Windows, macOS, and Linux. For more information.

**Step 1- Provision VPCs**

* Create 2 VPCs with name VPC1 and VPC 2
* Create 1 Subnet in each VPC with names Subnet1 in VPC1 and Subnet1 and VPC2
* Provision 2 internet gateway with names IGW1 and IGW2.

**Step 2- Provision EC2 instance and Security Groups**

* Create 2 security groups with name VPC1-EC2-SG and VPC2-EC2-SG
* Add inbound rule to open port 22 for SSH for 0.0.0.0/0
* Create 2 ec2 instances like EC2-One and EC2-Two
* Launch EC2-One in VPC1 with Public IP address.
* Launch EC2-Two in VPC2 without Public IP address.

**Step 3- Provision Transit Gateway**

**Step 4- SSH and Telnet**

* SSH into EC2-One using its Public IP address.
* Run such commands
  + Sudo yum update
  + Sudo yum install telnet
  + telnet<<EC2-Two Private IP address>> 22
* Able to telnet from EC1-One to EC2-Two via Transit Gateway