Project 10: Creating a VPC Peering Connection

Lab Overview

This lab demonstrates how to create a private VPC peering connection between two VPCs. VPC peering allows secure and private communication between resources in different VPCs. By the end of this lab, you will have established a peering connection, configured routing, enabled flow logs, and tested the connection.

Learning Objectives

By the end of this lab, students will be able to:

- Create a VPC peering connection between two VPCs.
- Configure route tables to utilize the VPC peering connection.
- Enable VPC Flow Logs to monitor network traffic.
- Test the VPC peering connection.
- Analyze VPC flow logs for traffic insights.

Requirements

- **Tools**: AWS Management Console and a web browser.

Lab Environment Setup

1. **Access AWS Console**: Log in to the AWS Management Console using the provided credentials.
2. **Ensure Proper Region**: Do not change the AWS region unless specifically instructed.

Tasks to Complete

Task 1: Creating a VPC Peering Connection

- Open the VPC Management Console and navigate to **Peering connections**.
- Create a new VPC peering connection with the following settings:
  - **Name**: `Lab-Peer`
  - **Requester VPC**: Lab VPC
  - **Accepter VPC**: Shared VPC
- After creating the peering connection, accept the request to establish the connection.

Task 2: Configuring Route Tables

- Update the route tables of both VPCs to route traffic through the peering connection:
  - For **Lab VPC**: Add a route that directs traffic destined for `10.5.0.0/16` (Shared VPC's CIDR block) to the `Lab-Peer` peering connection.
  - For **Shared VPC**: Add a route that directs traffic destined for `10.0.0.0/16` (Lab VPC's CIDR block) to the `Lab-Peer` peering connection.

Task 3: Enabling VPC Flow Logs

- Enable VPC Flow Logs to monitor traffic moving across the peered VPCs:
  - Navigate to **Shared VPC**, select **Flow Logs**, and create a flow log with the following settings:
    - **Name**: `SharedVPCLogs`
    - **Destination**: Send to CloudWatch Logs
    - **Log Group**: `ShareVPCFlowLogs`
    - **IAM Role**: `vpc-flow-logs-Role`

Task 4: Testing the VPC Peering Connection

- Test the VPC peering connection by configuring the inventory application to connect to the database in the Shared VPC.
- Access the application using the public IP of the EC2 instance in Lab VPC, then input the database connection details (endpoint, database name, username, and password).
- Verify that the application successfully connects to the database, indicating that the peering connection is functioning correctly.

Task 5: Analyzing the VPC Flow Logs

- Analyze the flow logs in CloudWatch to observe traffic patterns between the application and database.
- Look for log entries with port 3306, representing traffic between the application server and the database.

Lab Submission

- **Verification**: Take screenshots of each completed task, including the creation of the peering connection, route table configurations, VPC Flow Logs setup, and successful connection testing.
- **Submit**: Submit the screenshots along with a brief summary of your experience and what you learned.
- **Commands**: All the commands you have used in ".sh" file.

Important Notes

- Ensure all actions are performed in the correct AWS region as specified at the beginning of the lab.
- VPC peering connections do not support transitive routing; traffic can only flow between directly peered VPCs.

Additional Resources

- Amazon VPC Peering Documentation: Link
- AWS CloudWatch Logs Documentation: Link

Grading Criteria

- Successful creation and configuration of the VPC peering connection.
- Correct setup of route tables and flow logs.
- Evidence of successful testing and traffic analysis via flow logs.
- Clear and complete submission of screenshots and summary.