This lab demonstrates the steps from *Demo: Create a VPC.*
My full AWS Architect Associate course can be found here:
https://www.udemy.com/course/ultimateaws/?referralCode=7ED214B795C444141361

Lab Guide: Creating a Virtual Private Cloud (VPC) in AWS

This lab guide walks you through the basics of creating a Virtual Private Cloud (VPC) in the AWS Console. It follows the steps outlined in the material and explains key concepts along the way. By the end of this lab, you will understand how to create a secure and functional VPC for hosting resources in AWS.

Lab Objectives

1. Learn about the Default VPC and why it may not be suitable for secure workloads.
2. Create a custom VPC using AWS's "VPC and More" wizard.
3. Understand key VPC components, including CIDR ranges, subnets, NAT gateways, and VPC endpoints.

Step 1: Access the VPC Console

1. **Log into the AWS Console.**
2. Ensure you are in the **North Virginia (us-east-1)** region (or your desired region).
3. In the search bar at the top, type **VPC** and select the **VPC Console**.

Step 2: Understand the Default VPC

1. **Default VPC Overview**:
    - AWS creates a **Default VPC** in each region of your account.

    - This VPC includes default subnets, route tables, and an internet gateway.
2. **Security Consideration**:
    - The Default VPC is not highly secure by design and is intended for testing and basic use cases.
    - If not in use, consider deleting the Default VPC (only if no resources like EC2 instances or network interfaces are attached).

Step 3: Create a Custom VPC

1. Click on **Create VPC** in the VPC Console.
2. Select the **"VPC and More"** option for a simplified setup.

Step 4: Configure the Custom VPC

1. **Name Your VPC**:
    - Enter a name for your VPC (e.g., **DemoVPC**).
2. **Set the CIDR Range**:
    - Use the default range (e.g., `10.0.0.0/16`), which allows for 65,536 private IP addresses.
    - **Important**: Ensure this CIDR range does not overlap with any other VPCs or your on-premises network to avoid conflicts.
3. **Understand CIDR Ranges**:
    - CIDR ranges define the IP address space for the VPC.
    - Private IP ranges (e.g., `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`) are used for internal networking.

Step 5: Configure Subnets

1. **Availability Zones**:
    - Subnets will be automatically created in **two availability zones** for high availability.
    - Each subnet receives a portion of the VPC's CIDR range.
2. **Subnet Types**:
    - **Public Subnets**:
        - Designed for resources like web servers that need internet access.
        - Associated with an internet gateway.
    - **Private Subnets**:
        - For resources like databases and application servers that do not require direct internet access.
        - Use NAT gateways for outbound internet traffic.
        - The vast majority of workloads you create should be in Private Subnets.

Step 6: Add a NAT Gateway

1. **Purpose**:
    - Allows instances in private subnets to access the internet securely.
    - Prevents inbound traffic from reaching private instances.
2. **Create NAT Gateway**:
    - In the **NAT gateways ($)** section, select **In 1 AZ** in the setup wizard.
    - AWS will allocate an Elastic IP automatically.

Step 7: Add a VPC Endpoint for S3

1. **Purpose**:
    - Allows resources in your VPC to communicate with Amazon S3 directly, without sending traffic over the internet.
2. **Configuration**:
    - Enable the **S3 VPC Endpoint** option during the setup.

Step 8: Review and Create

1. **Review Configuration**:
    - Verify all settings: VPC name, CIDR range, subnets, NAT gateway, and VPC endpoint.
2. **Click Create VPC**:
    - AWS will handle the creation of associated resources, including:
        - Internet Gateway
        - Route Tables
        - Subnets
        - NAT Gateway
        - Elastic IP
3. **Monitor Progress**:
    - The process may take a few minutes as AWS sets up all resources.

Step 9: Verify Your VPC

1. Go to the **VPC Dashboard** and select your newly created VPC.
2. Review the components:
    - CIDR range
    - Subnets
    - Route tables
    - Internet gateway
    - NAT gateway
    - VPC endpoints

Key Concepts Explained

1. **VPC**:
    - Your isolated network in AWS where you can launch resources securely.
    - Provides control over IP address ranges, subnets, routing, and security.
2. **CIDR Range**:
    - Defines the pool of private IP addresses available within the VPC.
3. **Subnets**:
    - **Public Subnets**: Resources can communicate directly with the internet.
    - **Private Subnets**: Resources are isolated from the internet and rely on NAT gateways for outbound traffic.
4. **NAT Gateway**:
    - Allows private instances to securely access the internet.
5. **VPC Endpoint**:
    - Optimizes access to AWS services like S3 without internet exposure.

Step 10: Cleanup (Optional)

If you no longer need the VPC, you can delete it:

1. Terminate any resources (e.g., EC2 instances) using the VPC.
2. Delete subnets, NAT gateways, and route tables.
3. Finally, delete the VPC itself.

Summary

In this lab, you created a custom VPC using AWS's simplified "VPC and More" wizard. You learned about key VPC components, including CIDR ranges, subnets, NAT gateways, and VPC endpoints, and configured a secure environment for deploying AWS resources. By following this process, you can design VPCs tailored to your application's networking and security needs.