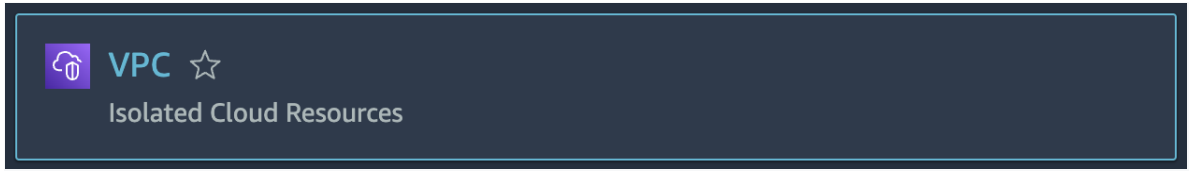
Introduction

In this lab step, you will create a private subnet. A common use case for private subnets is to configure resources for a back-end tier, such as database servers that should not be accessible from the internet. However, you may eventually want these back-end database servers to access the internet for operating system updates or to be accessible by administrators via a bastion host.

Instructions

1. In the AWS Management Console search bar, enter *VPC*, and click the **VPC** result under **Services**:



2. Select **cloudacademy-labs** in the **Filter by VPC** field.

3. Click **Subnets** in the left navigation pane. The Subnets page lists previously created subnets.

4. Click **Create Subnet** and specify the following details:

- **VPC ID**: Select the **cloudacademy-labs** VPC from the drop-down menu
- **Subnet name**: Enter *Private-A*
- **Availability Zone**: Select **us-west-2a**
- **CIDR block**: Enter *10.0.10.0/24* as the CIDR block of your subnet

5. Click **Create subnet**:

The created subnet is automatically attached to the default VPC Route table and the default Network ACL. Note that the CIDR block differs from the public subnet created previously. The third octet differs 10.0.10.0/24, not 10.0.20.0/24.

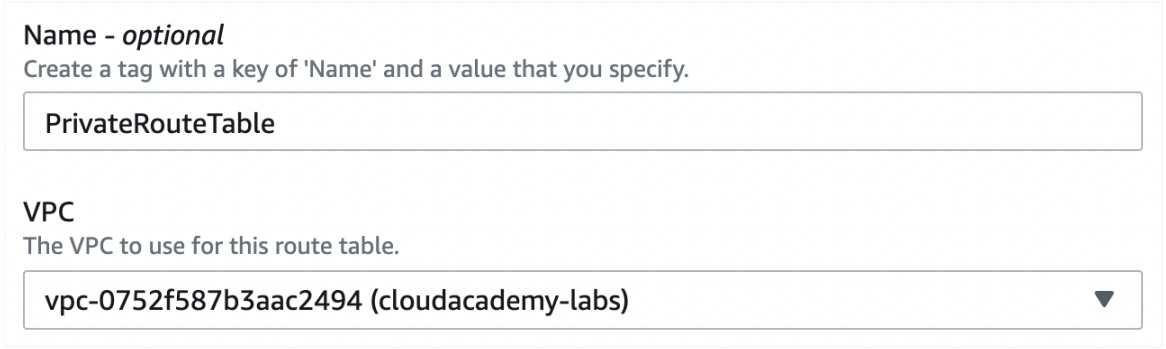
If a subnet does not have a route to the Internet (0.0.0.0/0) through a gateway, the subnet is known as a private subnet.

Next, you will create a custom private route table.

6. In the navigation pane, click **Route Tables**, then **Create route table** to open the dialog box:

7. Click **Create route table** and configure the following:

- **Name**: Enter *PrivateRouteTable*
- **VPC**: Select **cloudacademy-labs**

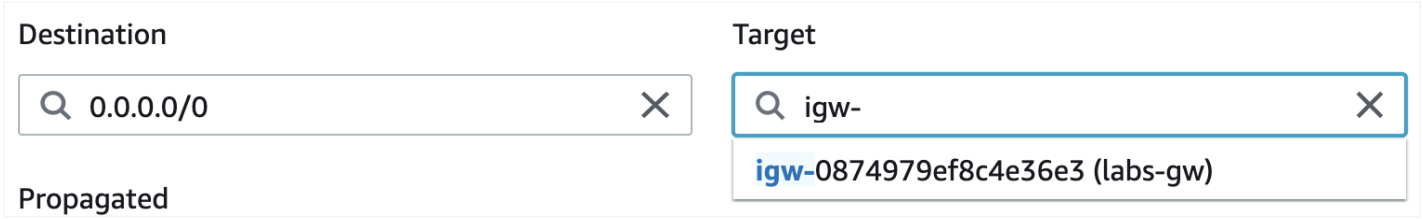


8. Click **Create route table**:

9. In the **PrivateRouteTable** details page, in the **Routes** tab, click **Edit routes**:

10. Click **Add route** and configure the following route settings:

- **Destination**: Enter *0.0.0.0/0*
- **Target**: Select **Internet Gateway**, then **labs-gw**



Important: This is a temporary target value. Later in this lab, you will add a NAT device (gateway or instance) and update the **Target** for the **PrivateRouteTable** to the NAT device. You are intentionally adding the NAT device last for learning purposes, which will require a minor change to the private route table once the NAT device is created and available.

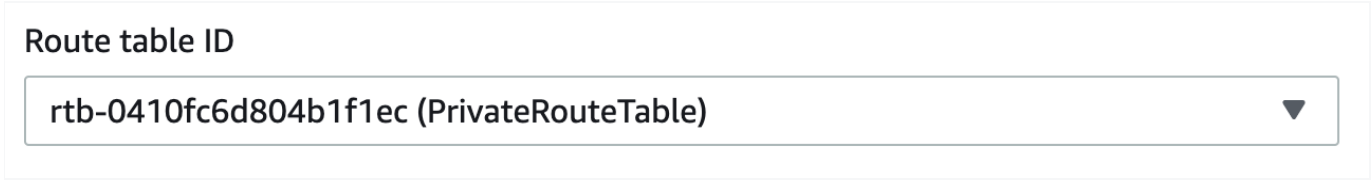
This route will eventually send traffic originating from your private subnet and bound for the public internet, to a NAT device.

11. Click **Save changes**:

12. Click **Subnets** from the left navigation pane, then select the **Private-A** subnet.

13. In the **Route Table** tab, and click **Edit route table association**:

14. Select **PrivateRouteTable** from the **Route table ID** drop-down menu:



15. Click **Save**:

Summary

In this lab, you created a private subnet and an associated route table. The route table currently has access to the public internet through the 0.0.0.0/0 route, but as mentioned before, you will update the target to a NAT device in a later lab step.

VALIDATION CHECKS

1 Checks

Check again

Created Subnets

Check if all the subnets have been created in the Lab environment

Amazon VPC