Introduction

A **Network Access Control List (NACL)** is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. The network access control list is a numbered list of rules, evaluated in order, to determine whether traffic is allowed in or out of any associated subnet. NACLs are stateless which means they cannot tell if a message is in response to a request that started *inside* the VPC, or if it is a request that started from the internet. Hence, a NACL is better suited for private subnets. For public subnets, using security groups is recommended without NACLs.

The VPC comes with a modifiable default network ACL and each subnet must be associated with a network ACL. If you do not explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL that allows all inbound and outbound traffic:

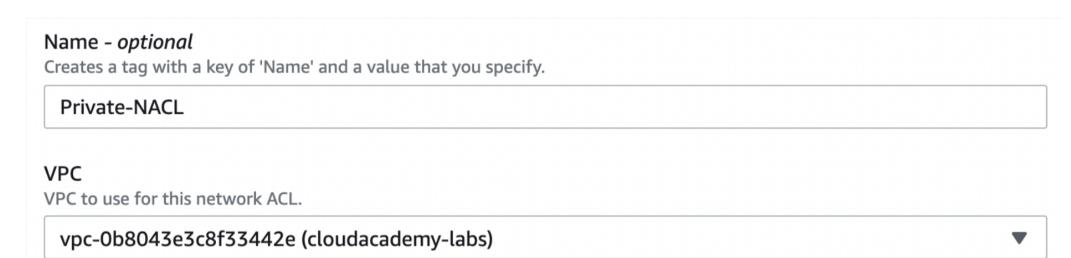In this lab, you will create a Network Access Control List for your private subnet.

Instructions

1. In the left navigation pane, click **Network ACLs** under **Security**:

2. Click **Create Network ACL**:

3. Configure the following Network ACL settings:

- **Name**: Enter *Private-NACL*
- **VPC**: Select **cloudacademy-labs** from the drop-down menu

Name - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

```
Private-NACL
```

VPC

VPC to use for this network ACL.

```
vpc-0b8043e3c8f33442e (cloudacademy-labs)          ▼
```

4. Click **Create network ACL**

Create network ACL

5. Select **Private-NACL** from the Network ACLs list and click the **Subnet associations** tab:

Subnet associations

6. Click **Edit subnet associations**:

Edit subnet associations

7. Select the check box for the **Private-A** subnet to associate it with the network ACL:

| ☑ | Private-A | subnet-084f6398046222d93 | acl-0e3d7023360579e86 | us-west-2a | 10.0.10.0/24 | – |

Selected subnets

subnet-084f6398046222d93 / Private-A ✕

Cancel　　**Save changes**

8. Click **Save changes**.

Summary

In this lab step, you created a Network ACL and associated it with the private subnet in your VPC.

VALIDATION CHECKS

1	**Checks**	Check again ⟳

✓ **Associated Network ACL with the Private Subnet**

Attached the Network ACL with the Private Subnet

Security for AWS