**Redshift Exercise: Create Security Group**

**Create Security Group for Redshift**

In this exercise, you'll create a security group you will later use to authorize access to your Redshift cluster.

A security group will act as firewall rules for your Redshift cluster to control inbound and outbound traffic.

1. Navigate to the [EC2 service](https://console.aws.amazon.com/ec2)

A screenshot of a computer program

Description automatically generated

Navigate to any service

1. Under **Network and Security** in the left navigation pane, select **Security Groups**. Click the **Create Security Group** button to launch a wizard.

A screenshot of a computer

Description automatically generated

Create a new security group

1. In the *Create security group* wizard, enter the basic details.

| **Section** | **Field** | **Value** |
| --- | --- | --- |
| Basic details | Security group name | redshift\_security\_group |
|  | Description | Authorise redshift cluster access |
|  | VPC | Choose the default VPC It is a VPC in a default region,  and has a public subnet in each Availability Zone. If a default VPC doesn't show up, [create a default VPC](https://docs.aws.amazon.com/vpc/latest/userguide/default-vpc.html#create-default-vpc) |

A screenshot of a computer

Description automatically generated

Create a default VPC, if not available already

A screenshot of a computer

Description automatically generated

Info about a default VPC

A screenshot of a computer

Description automatically generated

Basic details

1. In the *Inbound rules* section, click on **Add Rule** and enter the following values:

| **Section** | **Field** | **Value** |
| --- | --- | --- |
| Inbound rules | Type | Custom TCP Rule |
|  | Protocol | TCP |
|  | Port range | 5439 The default port for Amazon Redshift is 5439,  but your port might be different. |
|  | Source type | Custom |
|  | Source | 0.0.0.0/0 *(Anywhere in the world)* |

       >\*\*Important: Using `0.0.0.0/0` is not recommended for anything other than demonstration purposes because it allows access from any computer on the internet.\*\* In a real environment, you would create inbound rules based on your own network settings.

A screenshot of a computer

Description automatically generated

Inbound rules

1. Outbound rules allow traffic to anywhere by default.

A screenshot of a computer

Description automatically generated

Outbound rules

1. Click on the *Create security group* button at the bottom. You will see a success message.

A screenshot of a computer

Description automatically generated

Details of a security group