Day 2 - Create Security Group

The Nautilus DevOps team is strategizing the migration of a portion of their infrastructure to the AWS cloud. Recognizing the scale of this undertaking, they have opted to approach the migration in incremental steps rather than as a single massive transition. To achieve this, they have segmented large tasks into smaller, more manageable units. This granular approach enables the team to execute the migration in gradual phases, ensuring smoother implementation and minimizing disruption to ongoing operations. By breaking down the migration into smaller tasks, the Nautilus DevOps team can systematically progress through each stage, allowing for better control, risk mitigation, and optimization of resources throughout the migration process.

For this task, create a security group under default VPC with the following requirements:

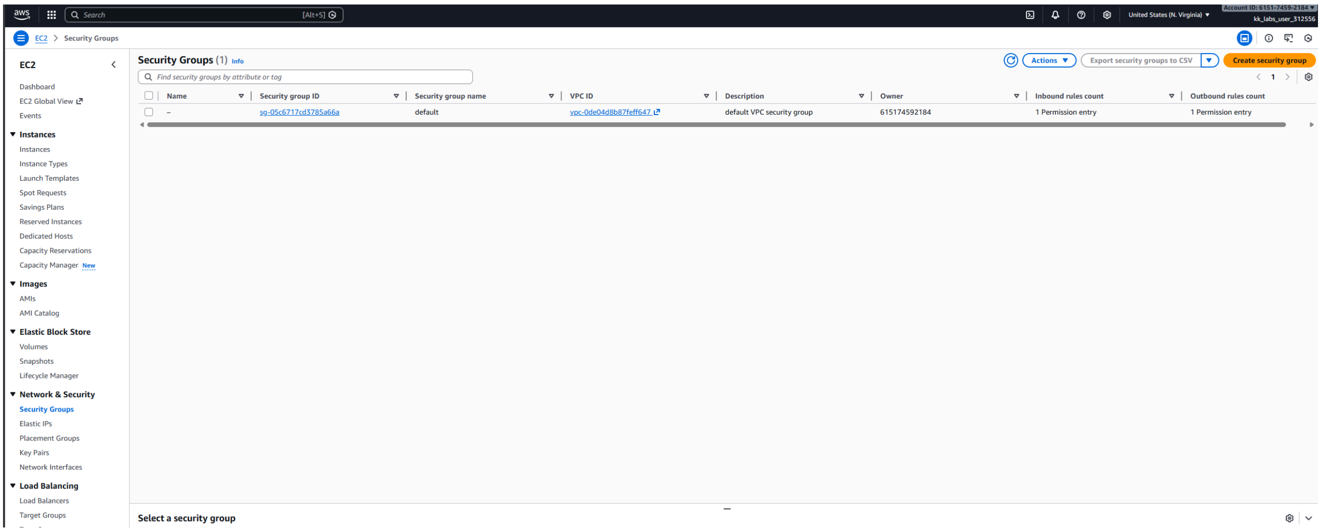
- Name of the security group is `xfusion-sg`.
- The description must be `Security group for Nautilus App Servers`
- Add the inbound rule of type `HTTP`, with port range of `80`. Enter the source CIDR range of `0.0.0.0/0`.
- Add another inbound rule of type `SSH`, with port range of `22`. Enter the source CIDR range of `0.0.0.0/0`.

What is an AWS Security Group?

An AWS Security Group acts as a virtual firewall that controls inbound and outbound traffic for your EC2 instances. Security groups use allow rules to permit specific traffic, and by default, deny all inbound traffic while allowing all outbound traffic. They operate at the instance level and provide stateful filtering, meaning return traffic is automatically allowed regardless of outbound rules.

Solution

First we need to head to EC2 > Network & security > Security Groups



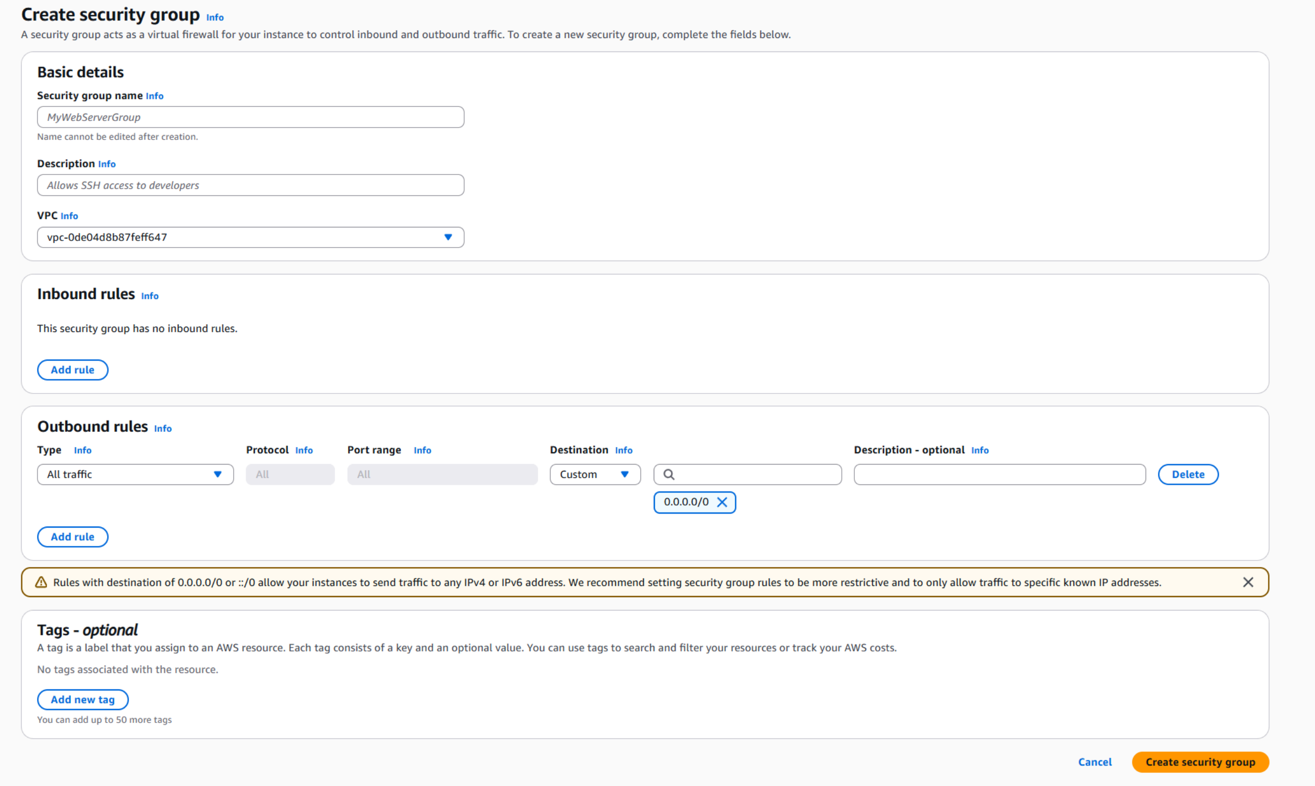
Security Groups (1) Info

Find security groups by attribute or tag

□	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
□	–	sg-05c6717cd3785a66a	default	vpc-0de04d8b87feff647	default VPC security group	615174592184	1 Permission entry	1 Permission entry

Select a security group

Click `Create Security Group`



Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name: MyWebServerGroup

Name cannot be edited after creation.

Description: Allows SSH access to developers

VPC: vpc-0de04d8b87feff647

Inbound rules

This security group has no inbound rules.

Outbound rules

Type	Protocol	Port range	Destination		Description - optional
All traffic	All	All	Custom	0.0.0.0/0	

Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

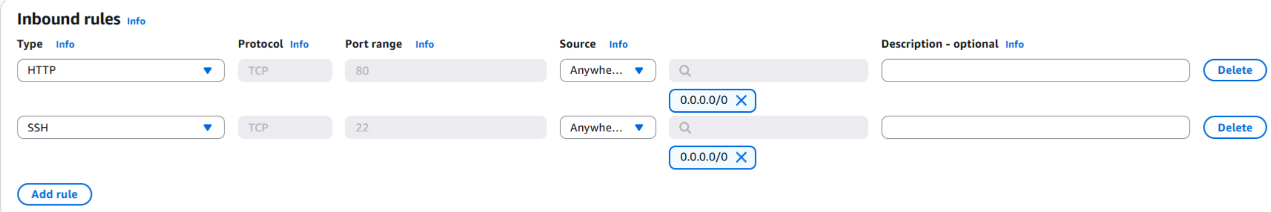
No tags associated with the resource.

You can add up to 50 more tags

Now we need to fill out all the fields with the requirements from earlier

Adding the first inbound rule we need to set the type to HTTP and then set the source to anywhere

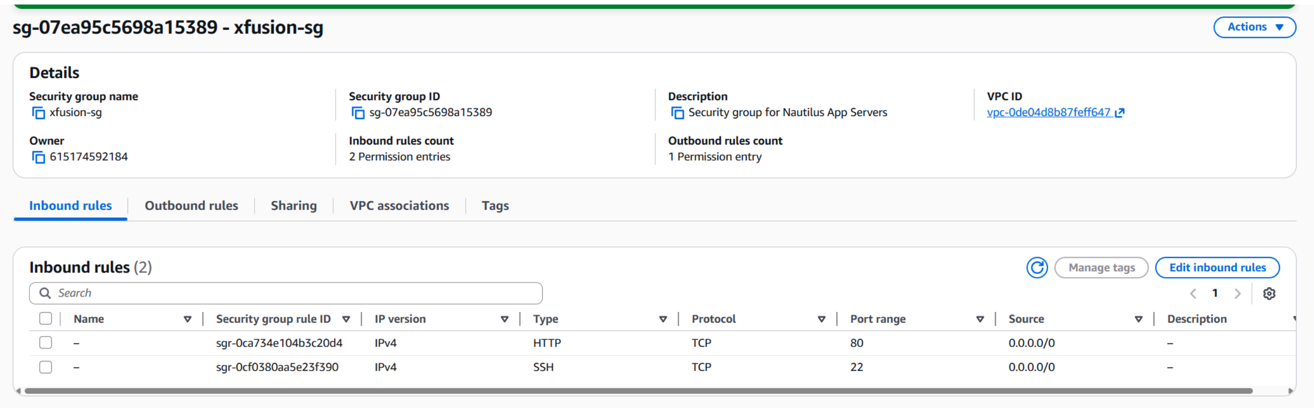
Now we need to add another inbound rule, which the type will be SSH with the source being anywhere



Inbound rules

Type	Protocol	Port range	Source		Description - optional
HTTP	TCP	80	Anywhe...	0.0.0.0/0	
SSH	TCP	22	Anywhe...	0.0.0.0/0	

After we have done this we now create the security group and we can now view it in the console



sg-07ea95c5698a15389 - xfusion-sg

Details

Security group name	Security group ID	Description	VPC ID
xfusion-sg	sg-07ea95c5698a15389	Security group for Nautilus App Servers	vpc-0de04d8b87feff647
Owner	**Inbound rules count**	**Outbound rules count**	
615174592184	2 Permission entries	1 Permission entry	

Inbound rules (2)

□	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-0ca734e104b3c20d4	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-0cf0380aa5e23f390	IPv4	SSH	TCP	22	0.0.0.0/0	–

Security Best Practices Implemented

✅ **Principle of Least Privilege**

✅ **Default Deny Approach**

✅ **Stateful Firewall**

Additional Recommendations

- SSH Access Hardening
- Web Traffic Protection
- Network Segmentation