

# Day 2 – Create Security Group (AWS)

## Challenge

### 100 Days of Cloud – AWS Track

#### Day 2 – Networking & Security Fundamentals

---

## 🎯 Objective

Create an **AWS Security Group** in the default VPC to control inbound traffic for application servers.

This task demonstrates understanding of **AWS network security**, inbound traffic rules, and region-specific resource creation.

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 `devops-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`.

Use below given AWS Credentials: (You can run the `showcreds` command on `aws-client` host to retrieve these credentials)

Console URL	<code>https://121244664515.signin.aws.amazon.com/console?region=us-east-1</code>
Username	<code>kk_labs_user_115760</code>
Password	<code>SIOI@3l8x@R6</code>
Start Time	Sat Dec 27 01:54:29 UTC 2025
End Time	Sat Dec 27 02:54:29 UTC 2025

**Notes:**

- Create the resources only in `us-east-1` region.
- To `display` or `hide` the terminal of the AWS client machine, you can use the expand toggle button as shown below:

Task 56:55 ⓘ

Check Try Later



## Task Requirements

Requirement	Value
Security Group Name	devops-sg
Description	Security group for Nautilus App Servers
VPC	Default VPC
Region	us-east-1
Inbound Rule 1	HTTP – Port 80 – Source 0.0.0.0/0
Inbound Rule 2	SSH – Port 22 – Source 0.0.0.0/0

## Concept Overview

An **AWS Security Group** acts as a virtual firewall that controls inbound and outbound traffic for AWS resources such as EC2 instances.

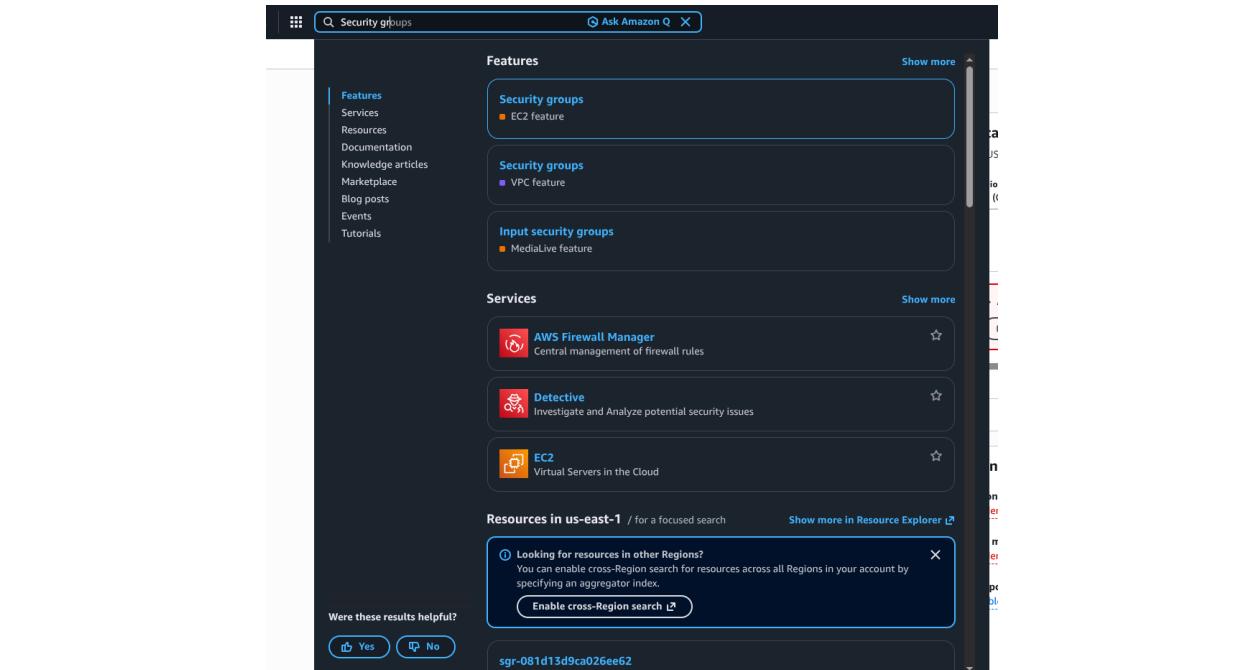
- Rules are **stateful**
  - Only allowed traffic is permitted
  - Commonly used to control application and administrative access
- 



## Implementation (AWS Management Console)

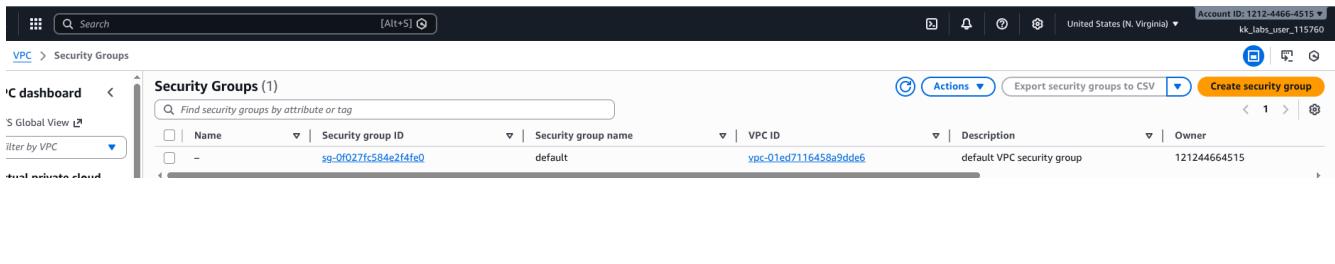
### Step 1: Log in to AWS Console

- Logged in to the AWS Management Console using the provided credentials
- Confirmed the region is set to **us-east-1**



## Step 2: Navigate to Security Groups

- Used the search bar to find **VPC**
- Clicked on **Security Groups** under the VPC service



## Step 3: Create a New Security Group

- Clicked **Create security group**
- Selected **Default VPC**
- Entered the following details:
  - Name:** devops-sg
  - Description:** Security group for Nautilus App Servers

## Step 4: Configure Inbound Rules

Added the following inbound rules:

- **HTTP**
  - Port: 80
  - Source: 0.0.0.0/0
- **SSH**
  - Port: 22
  - Source: 0.0.0.0/0

The screenshot shows the 'Create security group' page in the AWS VPC console. The 'Basic details' section includes a 'Security group name' field with 'devops-sg', a 'Description' field with 'Security group for Nautilus App Servers', and a 'VPC' field set to 'vpc-01ed7116458a9dde6'. The 'Inbound rules' section contains two entries: one for HTTP (TCP port 80) and one for SSH (TCP port 22), both with 'Anywhere' source and no specific IP ranges. A warning message at the bottom states: '⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

## Step 5: Create Security Group

- Reviewed all configuration details
- Clicked **Create security group**

### ✓ Outcome

- Successfully created a security group named devops-sg
- Configured HTTP and SSH access from all IP addresses
- Security group is ready to be attached to EC2 instances

## Key Takeaways

- Security Groups control inbound and outbound traffic in AWS
  - Proper rule configuration is critical for accessibility and security
  - Region selection matters when creating AWS resources
- 

## Proof of Work

This task demonstrates hands-on experience with: - AWS VPC and Security Groups - Network access control using inbound rules - AWS Console navigation and configuration

Screenshots included provide visual proof of real AWS console work.

---

**Next:** Day 3 – Create Subnet