Day 2 – Create Security Group (AWS)

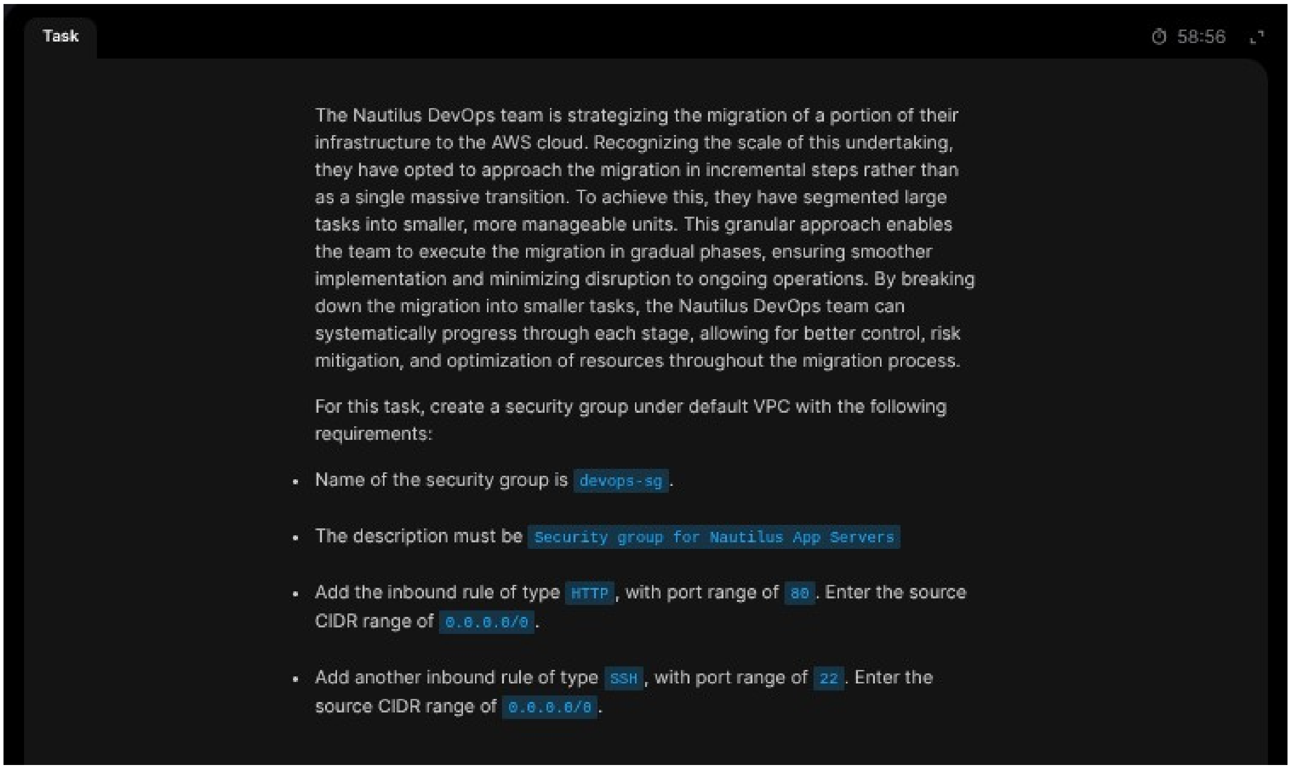
Challenge

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`.

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

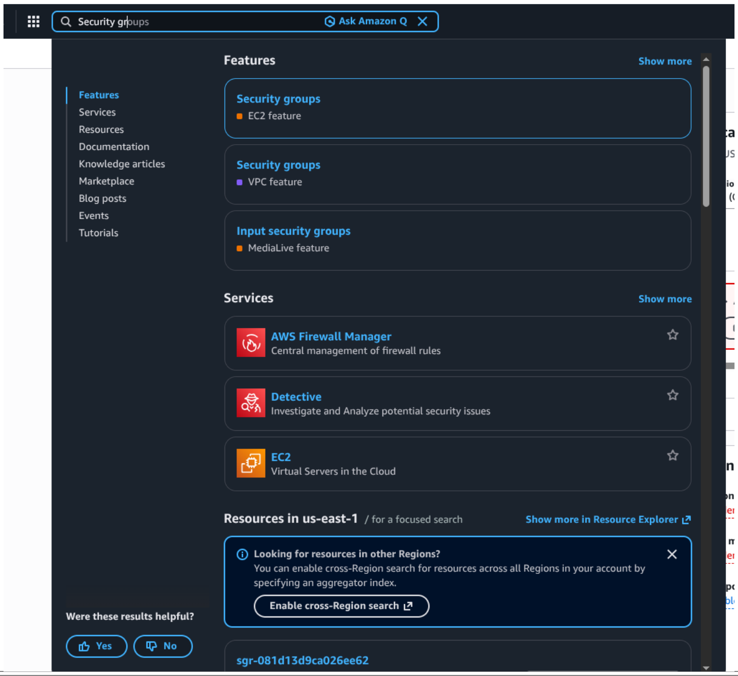
An **AWS Security Group** acts as a virtual firewall that controls inbound and outbound traffic for AWS resources such as EC2 instances.

- 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**



Security groups | Ask Amazon Q

Features | Show more

- Security groups — EC2 feature
- Security groups — VPC feature
- Input security groups — MediaLive feature

Services | Show more

- AWS Firewall Manager — Central management of firewall rules
- Detective — Investigate and Analyze potential security issues
- EC2 — Virtual Servers in the Cloud

Resources in us-east-1 / for a focused search | Show more in Resource Explorer

Looking for resources in other Regions?
You can enable cross-Region search for resources across all Regions in your account by specifying an aggregator index.

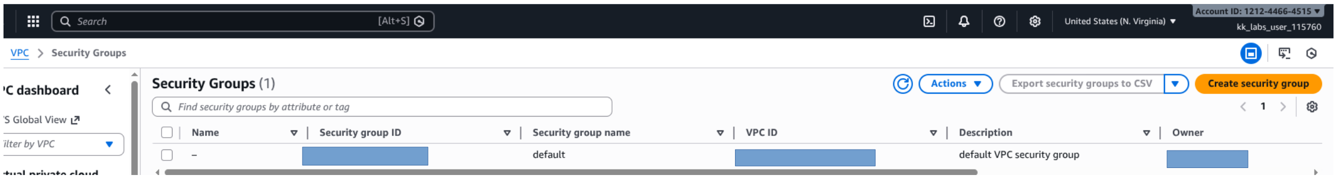
Enable cross-Region search

Were these results helpful?

sgr-081d13d9ca026ee62

Step 2: Navigate to Security Groups

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



Search [Alt+S]

United States (N. Virginia) | Account ID: 1212-4466-4515 | kk_labs_user_115760

VPC > Security Groups

Security Groups (1)

Find security groups by attribute or tag

Name	Security group ID	Security group name	VPC ID	Description	Owner
–	[redacted]	default	[redacted]	default VPC security group	[redacted]

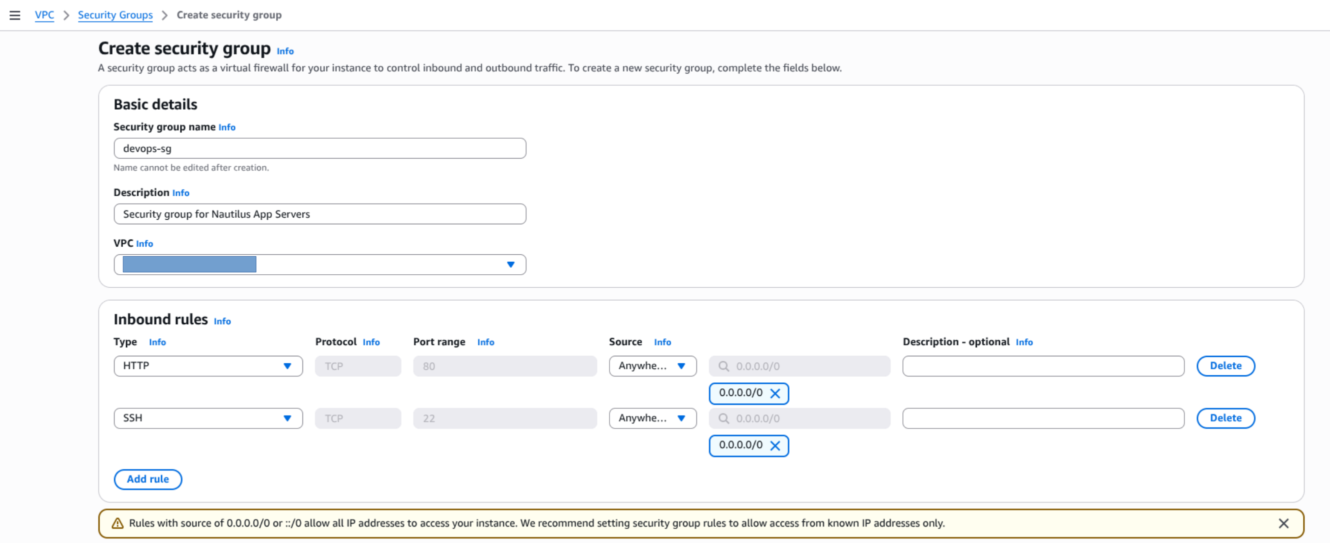
Step 3: Create a New Security Group

- 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



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: devops-sg

Name cannot be edited after creation.

Description: Security group for Nautilus App Servers

VPC: [redacted]

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	

⚠ 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