



◀ DevOps Lifecycle DevOps Roadmap Docker Tutorial Kubernetes Tutorials Amazon Web Services [AWS] Tutorial AZURE Tutorials GCP Tutorials ▶

Content Improvement
Event

Share Your Experiences

What is Security
Group in AWS and
How to Create it?

How to create an IAM
user in AWS

How To Create
Autoscaling Group In
AWS Using Terraform ?

How to Create AWS
Instance Scheduler ?

How to Create AWS
Access key and Secret
key?

How To Create Redhat
EC2 Instance in AWS

What is Security Group in AWS and How to Create it?

Last Updated : 17 Jun, 2024



Cybersecurity has grown to be a crucial component of any business in the modern digital age. Access management is a fundamental element of cybersecurity. Controlling access includes deciding who has access to what resources and for what goals. The management of resource access in the cloud is done using security groups. We shall define security groups in this article and explain how they operate and may be created in Amazon Web Services (AWS). We'll also define a few crucial terms related to security groups, offer pertinent examples, and give step-by-step directions with screenshots.

An example of one of these features is the security group, which functions as a virtual firewall to regulate the inbound and

Skip to content



[Amazon EC2 instances](#) or other AWS resources in a VPC. We shall go over a security group's definition and formation in this article.

1. **Security Group:** It performs the function of a virtual firewall, managing the inbound and outbound traffic for one or more Amazon EC2 instances or other AWS services within a [VPC](#).
2. **Inbound Rules:** These outline the types of traffic that are permitted to use the resources. It serves as a virtual firewall, controlling the traffic going in and coming out of a VPC for one or more Amazon EC2 instances or other AWS services.
3. **Outbound Rules:** These regulate the traffic that is permitted to depart from the resources. The destination for incoming traffic is dealt with by outbound rules. They may be forwarded to an alternative [Security Group](#), a [CIDR block](#), a single [IPv4 or IPv6 address](#), or all three.
4. **Amazon EC2:** A web service called Amazon Elastic Compute Cloud offers scalable computation capability in the cloud. For developers, it is intended to make web-scale cloud computing simpler.

[Skip to content](#)

5. **VPC:** A virtual network called a virtual private cloud enables you to launch Amazon resources into a defined virtual network.
6. **CIDR:** A technique for allocating IP addresses and rerouting Internet Protocol packets is called classless inter-domain routing (CIDR).
7. **Protocol:** A protocol is a collection of guidelines that controls how two devices communicate with one another.
8. **Port:** A port on a computer serves as the communication endpoint for a particular process or service.

Steps to Create a Security Group

Let's talk about how to form a security group in AWS now that we have identified certain critical terms.

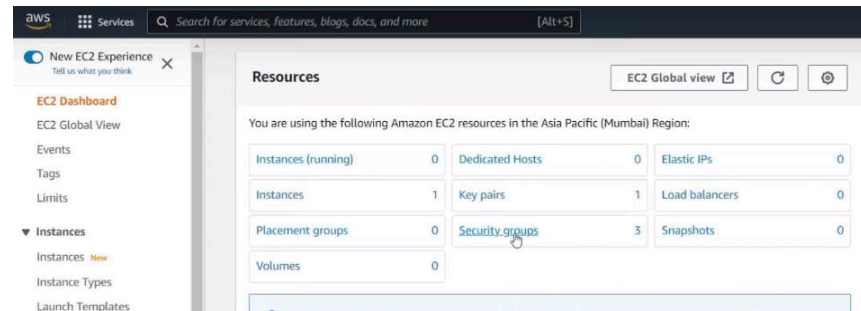
Step1: Access the EC2 Dashboard

Begin by logging into the [Amazon Management Console](#). Navigate to the AWS console and sign in with your account credentials.

Step 2: Navigate to Security Groups

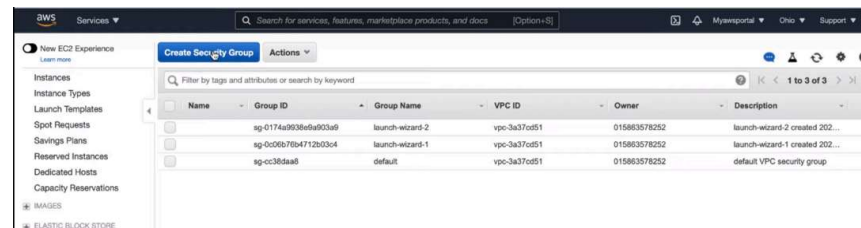
[Skip to content](#)

From the AWS console, go to the EC2 dashboard.
On the left-hand panel, locate and select the
“Security Groups” option.



Step 3: Initiate Security Group Creation

Within the “Security Groups” section, click on the
“Create Security Group” button to start the creation
process.



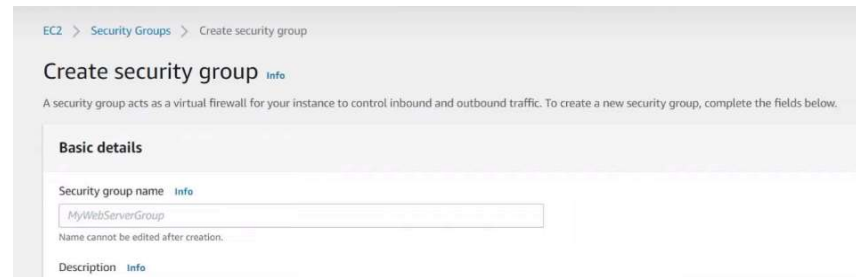
Step 4: Define Security Group Details

[Skip to content](#)

Provide the necessary details for your security group.

Enter a descriptive name and a brief description.

Specify the Virtual Private Cloud (VPC) where the security group will reside.



EC2 > Security Groups > Create security group

Create security group Info

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 Info

MyWebServerGroup

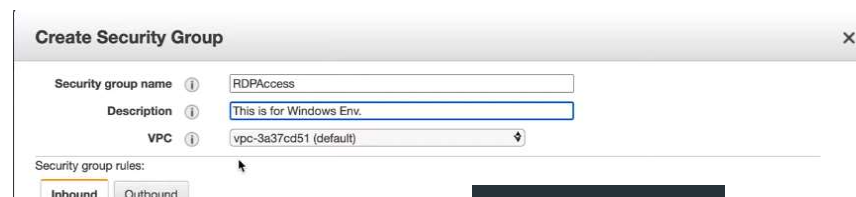
Name cannot be edited after creation.

Description Info

Insert your security group's information, including its name, description, and VPC. For your security group, you must also provide inbound and outgoing rules.

Step 5: Configure Inbound Rules

To define inbound rules, select the “Inbound Rules” tab and click on the “Add Rule” button. Configure each rule by specifying the protocol, port range, source IP address or range, and a description.



Create Security Group

Security group name Info RDPAAccess

Description Info This is for Windows Env.

VPC Info vpc-3a37cd51 (default)

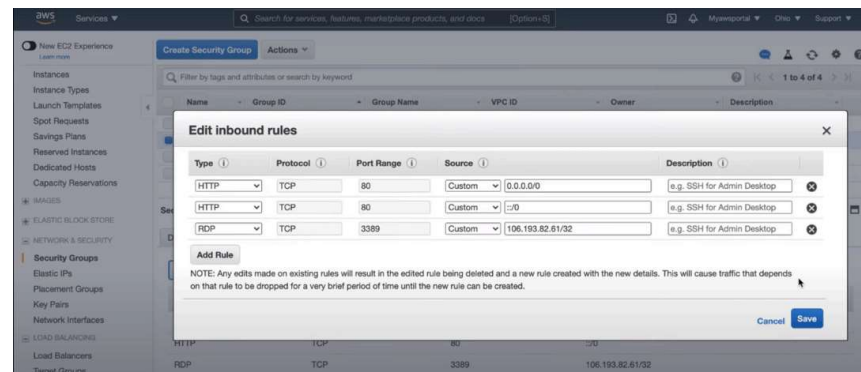
Security group rules:

Inbound Outbound

Skip to content

Step 6: Configure Outbound Rules

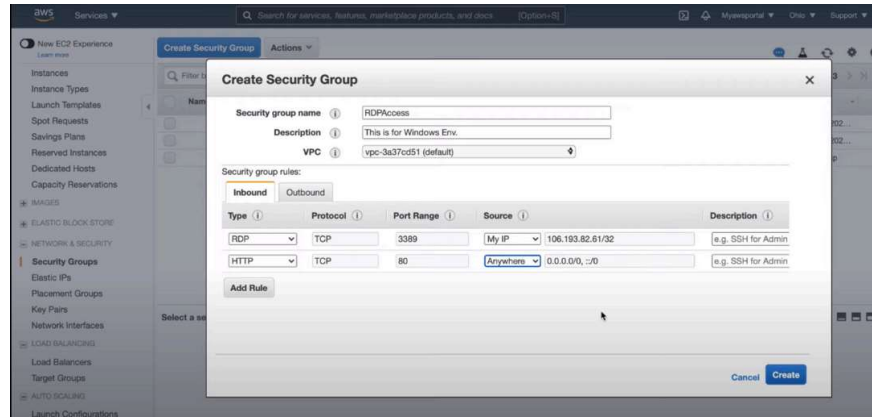
Similarly, configure outbound rules by selecting the “Outbound Rules” tab and clicking on the “Add Rule” button. Define the protocol, port range, destination IP address, and a description for each rule.



Step 7: Review and Create

[Skip to content](#)

Carefully review all the configurations and rules you have set up. Once satisfied, click on the “Create Security Group” button to finalize and create your security group.



- **Note:** Inbound and outbound security Group Rules comprise four different fields: **Source**, **Protocol**, **Port Range** & **Description**.
- **Source:** Typically, this is a private IP address, a subnet mask, or another security group. If you use the “anywhere (0.0.0.0/0)” option, you can also allow access to the entire internet. The everywhere (0.0.0.0/0) value must only be used when necessary, and you should be well aware of the risks involved.
- **Protocol:** TCP is usually the default protocol and is often greyed out. But you can adjust the

[Skip to content](#)

protocols if you're using specially-made rules that you wrote.

- **Port Range:** Usually, port ranges are pre-filled. Still, you have the option to choose a custom port range of your choice.
- **Description:** You can add a description to the rule you've generated in this area. The more specific you are, the better.

Amazon EC2 security groups for Linux instances

Amazon EC2 security groups play a pivotal role in [safeguarding Linux instances](#) hosted on the Amazon Web Services (AWS) cloud platform. They serve as virtual firewalls, controlling inbound and outbound traffic to and from EC2 instances. Understanding how to configure and manage security groups is essential for maintaining a secure and efficient computing environment. In this detailed guide, we'll delve into the intricacies of Amazon EC2 security groups for [Linux instances](#).

Understanding EC2 Security Groups:

Skip to content

- **Definition:** EC2 security groups act as virtual firewalls that regulate traffic to and from EC2 instances. They control inbound traffic (incoming data) and outbound traffic (outgoing data) based on defined rules.
- **Stateful Filtering:** Security groups operate on a stateful filtering paradigm, meaning that responses to allowed inbound traffic are automatically allowed, regardless of outbound rules. This simplifies configuration and ensures that return traffic is permitted.
- **Default Rules:** By default, all inbound traffic is denied, and all outbound traffic is allowed. You must explicitly define inbound rules to permit traffic to your instances. Outbound traffic is automatically allowed unless specific restrictions are imposed.

Change, or Delete Security Groups

Managing security groups in AWS is a crucial aspect of maintaining a secure and compliant cloud environment. Whether you need to update rules, modify associations, or remove unused security groups, the process is straightforward. Here's a

[Skip to content](#)

simple guide on how to change or delete security groups in AWS:

Changing Security Groups:

- **Access the AWS Management Console:** Log in to the AWS Management Console and navigate to the EC2 dashboard.
- **Locate Security Groups:** From the EC2 dashboard, select the “Security Groups” option from the navigation pane to view all existing security groups.
- **Identify Target Security Group:** Identify the security group you wish to modify and click on its name to access its configuration details.
- **Update Security Group Rules:** Within the security group details, navigate to the “Inbound” or “Outbound” rules tab to modify existing rules. Click on the “Edit” button to make changes, such as adding new rules, modifying existing ones, or removing unnecessary rules.
- **Review and Apply Changes:** Carefully review the updated rules to ensure they align with your security requirements. Once satisfied, click on the “Save” or “Apply Changes” button to implement the modifications.

Skip to content

Deleting Security Groups:

- **Access the AWS Management Console:** Follow the same initial steps to access the EC2 dashboard in the AWS Management Console.
- **Locate Security Groups:** From the EC2 dashboard, select the “Security Groups” option to view a list of all existing security groups.
- **Identify Target Security Group:** Identify the security group you intend to delete from the list of available security groups.
- **Initiate Deletion:** Select the target security group and click on the “Actions” dropdown menu. Choose the “Delete Security Group” option from the available actions.
- **Confirm Deletion:** AWS will prompt you to confirm the deletion of the selected security group. Review the details and implications of the deletion carefully.
- **Confirm Deletion:** If you’re certain you want to proceed with the deletion, click on the “Yes, Delete” button to confirm. Otherwise, you can cancel the operation to retain the security group.

Conclusion

[Skip to content](#)

Security groups are a fundamental security feature in AWS, allowing you to control the traffic that is allowed to access your resources. In this article, we have discussed what a security group is and how to create it. By following the steps mentioned above, you can create security groups for your resources and ensure they are secure.

Security Group in AWS – FAQs

What is an AWS security group?

An AWS security group acts as a virtual firewall for controlling inbound and outbound traffic to AWS resources, such as EC2 instances, based on defined rules. It regulates access by allowing or denying traffic based on specified protocols, ports, and [IP addresses](#).

What is AWS security group vs NACL?

[Skip to content](#)

AWS security groups are stateful firewalls that control inbound and outbound traffic to AWS instances, while [Network Access Control Lists \(NACLs\)](#) are stateless firewalls that [filter traffic](#) at the subnet level in AWS.

How many security groups are there in AWS?

In AWS, you can create up to 500 security groups per VPC (Virtual Private Cloud) to control inbound and outbound traffic for your instances. Each security group can contain multiple rules to manage access.

What is the default security group in AWS?

The default security group in AWS allows all outbound traffic and denies all inbound traffic by default. It's automatically associated with

Skip to content

any EC2 instance launched in a VPC unless another security group is explicitly specified.

What is the purpose of a security group?

The purpose of a security group is to act as a virtual firewall, controlling inbound and outbound traffic to and from EC2 instances in AWS, thereby enhancing network security and access control.

Three 90 Challenge is back on popular demand! After processing refunds worth INR 1CR+, we are back with the offer if you missed it the first time. Get 90% course fee refund in 90 days. [Avail now!](#)

Are you looking to become an AWS Expert? Enroll in our [AWS Solutions Architect Certification Training Program](#) on GeeksforGeeks and take advantage of our Three 90 Challenge: Get a whopping **90% refund on course completion** within 90 Days.

Skip to content

Perfect for students and working professionals, this live course covers everything from foundational concepts to advanced AWS services, preparing you for the certification exam. With real-time training and hands-on projects, you'll gain the skills to design and deploy scalable applications on AWS.



Next Article >

How to create an IAM
user in AWS

Similar Reads

Amazon S3 And Security Standards In AWS Securi...

Storing important stuff online can be tricky, especially when you have tons of secrets and rules that you hav...

🕒 8 min read

Difference between Security Group and Network...

In AWS Cloud, Both the security groups and network ACLs play a important roles in managing the network...

🕒 8 min read

Skip to content

How To Create Spot Instance In Aws-Ec2 In Aws...

Spot instances are available at up to 90% discount because when instances are not used then the...

🕒 6 min read

How to create AWS s3 presigned url Using AWS...

Amazon Simple Storage Service or AWS S3 is a scalable object storage service that allows users to...

🕒 3 min read

How To Create Autoscaling Group In AWS Using...

An auto-scaling group is a service that is provided in EC2 and is primarily used for an automatic increase o...

🕒 7 min read

Difference between AWS Cloudwatch and AWS...

1. AWS Cloudwatch: It is a monitoring tool used for real-time monitoring of AWS resources and...

🕒 2 min read

AWS Educate and AWS Emerging Talent Community

If you want to make your career in cloud computing but don't know how to get started, [Skip to content](#) register for...

 2 min read

How To Deploy GraphQL API Using AWS Lambda...

GraphQL is known for its flexibility and efficiency. AWS Lambda, on the other hand, provides a...

 6 min read

Difference Between AWS (Amazon Web Services)...

While both AWS ECS and Fargate play in the container orchestration field, their approaches diverg...

 8 min read

AWS DynamoDB - Insert Data Using AWS Lambda

In this article, we will look into the process of inserting data into a DynamoDB table using AWS Lambda....

 3 min read

Article Tags :

[Amazon Web Services](#)[DevOps](#)[Network-security](#)[Skip to content](#)



Corporate & Communications Address:- A-143, 9th Floor, Sovereign Corporate Tower, Sector- 136, Noida, Uttar Pradesh (201305)
| Registered Address:- K 061, Tower K, Gulshan Vivante Apartment, Sector 137, Noida, Gautam Buddh Nagar, Uttar Pradesh, 201305



Company

- About Us
- Legal
- Careers
- In Media
- Contact Us
- Advertise with us
- GFG Corporate Solution
- Placement Training Program

Explore

- Job-A-Thon
- Hiring Challenge
- Hack-A-Thon
- GfG Weekly
- Contest
- Offline Classes (Delhi/NCR)
- DSA in JAVA/C++
- Master System
- Design
- Master CP
- GeeksforGeeks
- Videos
- Geeks
- Community

Languages

- Python
- Java
- C++
- PHP
- GoLang
- SQL
- R Language
- Android Tutorial

DSA

- Data Structures
- Algorithms
- DSA for Beginners
- Basic DSA
- Problems
- DSA Roadmap
- DSA Interview
- Questions
- Competitive Programming

Data Science & ML

- Data Science With Python
- Data Science For Beginner
- Machine Learning Tutorial
- ML Maths
- Data Visualisation Tutorial
- Pandas Tutorial
- NumPy Tutorial
- NLP Tutorial
- Deep Learning Tutorial

Web Technologies

- HTML
- CSS
- JavaScript
- TypeScript
- ReactJS
- NextJS
- NodeJs
- Bootstrap
- Tailwind CSS

Python Tutorial

Computer Science

DevOps

System Design

School Subjects

Commerce

- Accountancy
- Business Studies

Skip to content

Databases	Preparation	Competitive	More	Free Online	Write & Earn
SQL	Corner	Exams	Tutorials	Tools	Write an Article
MYSQL	Company-Wise	JEE Advanced	Software	Typing Test	Improve an
PostgreSQL	Recruitment	UGC NET	Development	Image Editor	Article
PL/SQL	Process	UPSC	Software Testing	Code Formatters	Pick Topics to
MongoDB	Resume	SSC CGL	Product	Code Converters	Write
	Templates	SBI PO	Management	Currency	Share your
	Aptitude	SBI Clerk	Project	Converter	Experiences
	Preparation	IBPS PO	Management	Random	Internships
	Puzzles	IBPS Clerk	Linux	Number	
	Company-Wise		Excel	Generator	
	Preparation		All Cheat Sheets	Random	
	Companies		Recent Articles	Password	
	Colleges			Generator	