

## Creating DB Instance


First of all sign up to AWS if you don't have an account yet.


Access RDS page: <https://us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#GettingStarted>.


Click on "Create database" and create as the example below:


### Engine options


Engine type [Info](#)


☐ Amazon Aurora  


☒ MySQL  


☐ MariaDB  



☐ PostgreSQL  


☐ Oracle  


☐ Microsoft SQL Server  


Edition

☒ MySQL Community

 **Known issues/limitations**  
Review the [Known issues/limitations](#) to learn about potential compatibility issues with specific database versions.

Version

MySQL 8.0.28 ▼

### Templates

Choose a sample template to meet your use case.

☐ **Production**  
Use defaults for high availability and fast, consistent performance.

☐ **Dev/Test**  
This instance is intended for development use outside of a production environment.

☒ **Free tier**  
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.  
[Info](#)


\*It's important saving your DB's: identifier, user, password, port and host (endpoint)

For a first try I recommend using this configurations, later you can understand more about it and do a better configuration for a more robust security.

It's easier to keep Public access as "yes" to use this project solution to storage data the with python.

Choose to create a new “VPC security group”, later we will configure it.


## Connectivity



**Virtual private cloud (VPC)** [Info](#)  
VPC that defines the virtual networking environment for this DB instance.

Default VPC (vpc-00a47fe4917cbad5b) ▼

Only VPCs with a corresponding DB subnet group are listed.

 After a database is created, you can't change its VPC.

**Subnet group** [Info](#)  
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default-vpc-00a47fe4917cbad5b ▼

**Public access** [Info](#)

☒ **Yes**  
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

☐ **No**  
RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

**VPC security group**  
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

☐ **Choose existing**  
Choose existing VPC security groups

☒ **Create new**  
Create new VPC security group

**New VPC security group name**

test-001

**Availability Zone** [Info](#)

No preference ▼

▼ **Additional configuration**

**Database port** [Info](#)  
TCP/IP port that the database will use for application connections.

3306

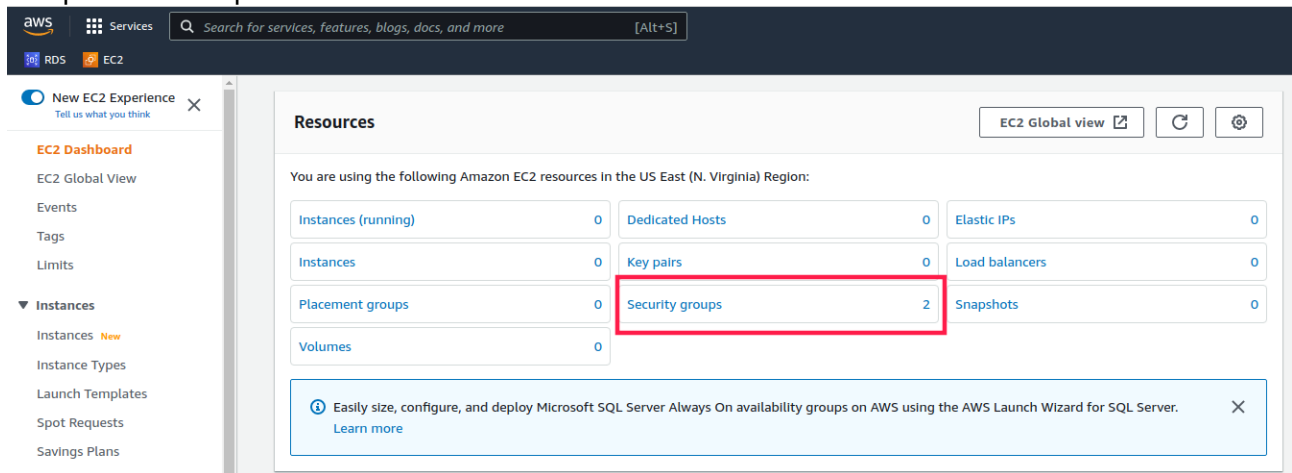
## Database authentication

### Database authentication options [Info](#)

- ☒ **Password authentication**  
Authenticates using database passwords.
- ☐ **Password and IAM database authentication**  
Authenticates using the database password and user credentials through AWS IAM users and roles.
- ☐ **Password and Kerberos authentication**  
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

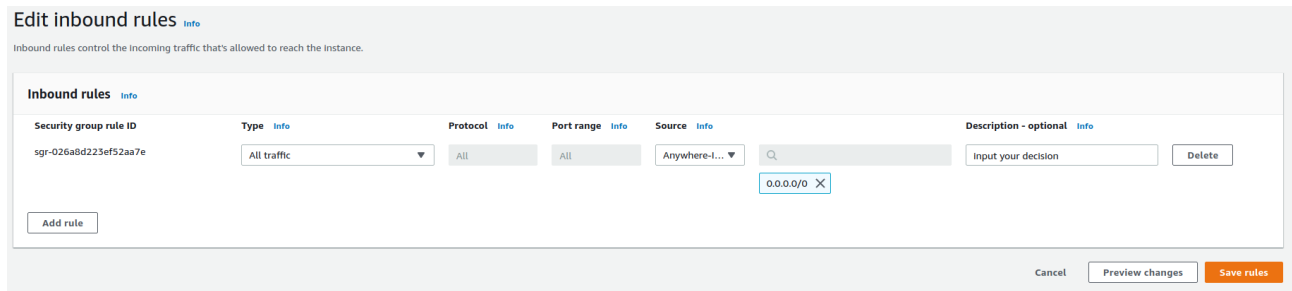
## Setting Security Group

Go to EC2 service page and look for “security groups” page. Select the group created in the previous step.



The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, 'Services', a search bar, and a '[Alt+S]' shortcut. The left sidebar shows the 'EC2' service selected, with a 'New EC2 Experience' prompt and a list of navigation options including 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', and 'Instances'. The 'Instances' section is expanded, showing 'Instances' (marked as 'New'), 'Instance Types', 'Launch Templates', 'Spot Requests', and 'Savings Plans'. The main content area is titled 'Resources' and shows a summary of EC2 resources in the US East (N. Virginia) Region. A table lists various resources with their counts: Instances (running) 0, Instances 0, Placement groups 0, Volumes 0, Dedicated Hosts 0, Key pairs 0, Security groups 2 (highlighted with a red box), Elastic IPs 0, Load balancers 0, and Snapshots 0. A blue notification banner at the bottom of the resources section provides information about Microsoft SQL Server Always On availability groups.

Allow “All traffic” and save.



The screenshot shows the 'Edit inbound rules' page for a security group. The page title is 'Edit inbound rules' with an 'Info' link. Below the title, a note states: 'Inbound rules control the incoming traffic that's allowed to reach the instance.' The main content area is titled 'Inbound rules' with an 'Info' link. It displays a table of inbound rules for the security group 'sgr-026a8d223ef52aa7e'. The table has columns for 'Security group rule ID', 'Type', 'Protocol', 'Port range', 'Source', and 'Description - optional'. The first rule is 'All traffic', which is selected. The 'Source' field is set to 'Anywhere-Internet' and is highlighted with a red box. Below the table, there is an 'Add rule' button. At the bottom right of the page, there are three buttons: 'Cancel', 'Preview changes', and 'Save rules' (highlighted in orange).