

To access RDS of cloud from local laptop

Step-1

You must have mySQL client(either command line or workbench) on your local Laptop

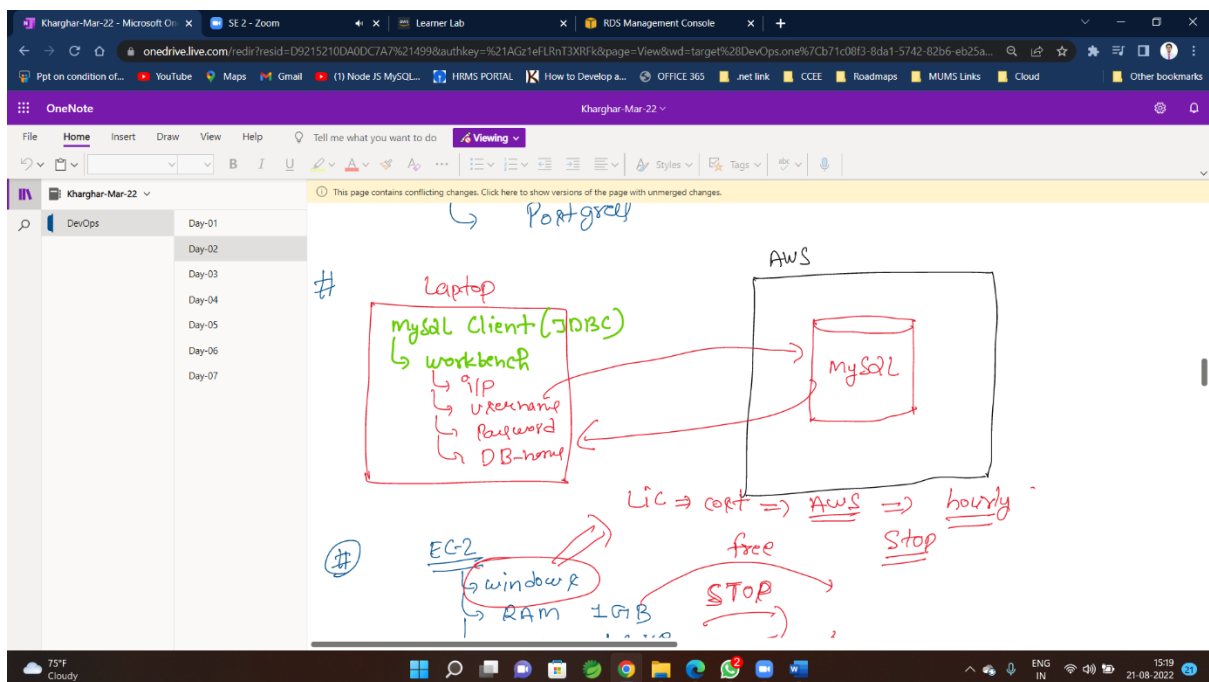
You need

1.i/p address

2.user name

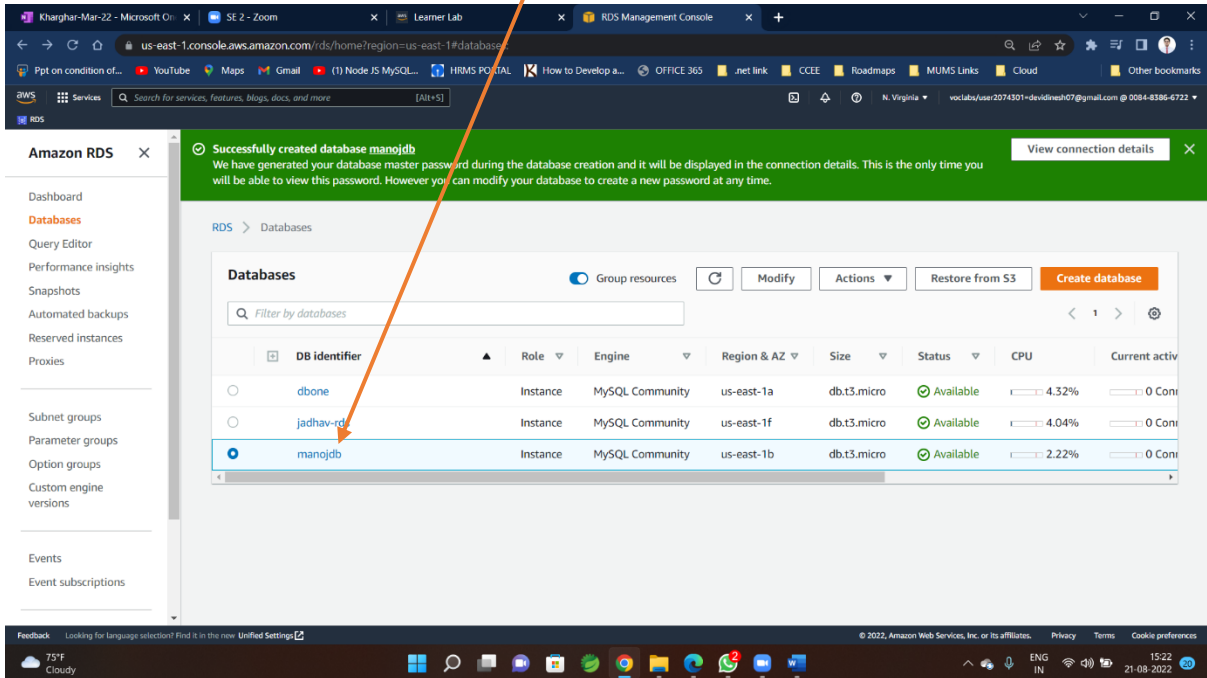
3.password

4.db name



Step-2

Click on database name to get credentials



The screenshot shows the Amazon RDS console interface. A green banner at the top indicates that a database named 'manojdb' was successfully created. Below this, the 'Databases' section is displayed, showing a table of database instances. An orange arrow points to the 'manojdb' entry in the 'DB identifier' column.

	DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activ
<input type="radio"/>	dbone	Instance	MySQL Community	us-east-1a	db.t3.micro	Available	4.32%	0 Con
<input type="radio"/>	jadhav-td	Instance	MySQL Community	us-east-1f	db.t3.micro	Available	4.04%	0 Con
<input checked="" type="radio"/>	manojdb	Instance	MySQL Community	us-east-1b	db.t3.micro	Available	2.22%	0 Con

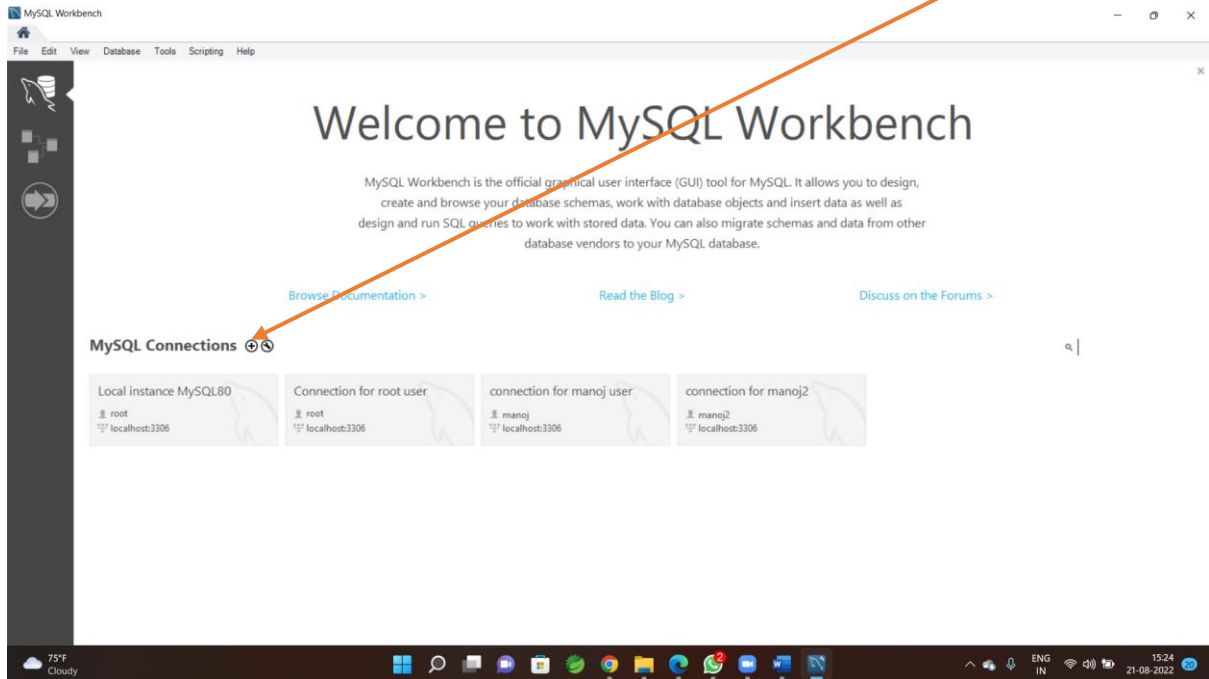
Step-3 copy Endpoint this will be the ip and port details given

The screenshot displays the AWS RDS console interface. The left sidebar contains navigation links for Dashboard, Databases, Query Editor, Performance insights, Snapshots, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Events, and Event subscriptions. The main content area is titled 'Connectivity & security' and includes tabs for Monitoring, Logs & events, Configuration, Maintenance & backups, and Tags. The 'Endpoint & port' section shows the Endpoint as `manojdb.cqpggf4m.us-east-1.rds.amazonaws.com` and the Port as 3306. The 'Networking' section lists the Availability Zone (us-east-1b), VPC (vpc-0a731d95fe38acf3a), Subnet group (default-vpc-0a731d95fe38acf3a), and Subnets (subnet-0c4395b11b35a59dd, subnet-0dc81ae990e1aa8e6, subnet-0001b2b44d32dd7b9, subnet-00d3269891208e793, subnet-02ce2bd49111be18d, subnet-027fe8e89eb6a1ce1). The 'Security' section shows the VPC security groups (mysql_rds (sg-0be30c3d455a7f49f) Active), Public accessibility (Yes), Certificate authority (rds-ca-2019), and Certificate authority date (August 22, 2024, 22:38 (UTC+05:30)). The bottom status bar indicates the date and time as 21-08-2022 15:21.

Section	Field	Value
Endpoint & port	Endpoint	manojdb.cqpggf4m.us-east-1.rds.amazonaws.com
	Port	3306
Networking	Availability Zone	us-east-1b
	VPC	vpc-0a731d95fe38acf3a
	Subnet group	default-vpc-0a731d95fe38acf3a
	Subnets	subnet-0c4395b11b35a59dd subnet-0dc81ae990e1aa8e6 subnet-0001b2b44d32dd7b9 subnet-00d3269891208e793 subnet-02ce2bd49111be18d subnet-027fe8e89eb6a1ce1
	Network type	IPv4
	Public accessibility	Yes
Security	VPC security groups	mysql_rds (sg-0be30c3d455a7f49f) Active
	Certificate authority	rds-ca-2019
	Certificate authority date	August 22, 2024, 22:38 (UTC+05:30)

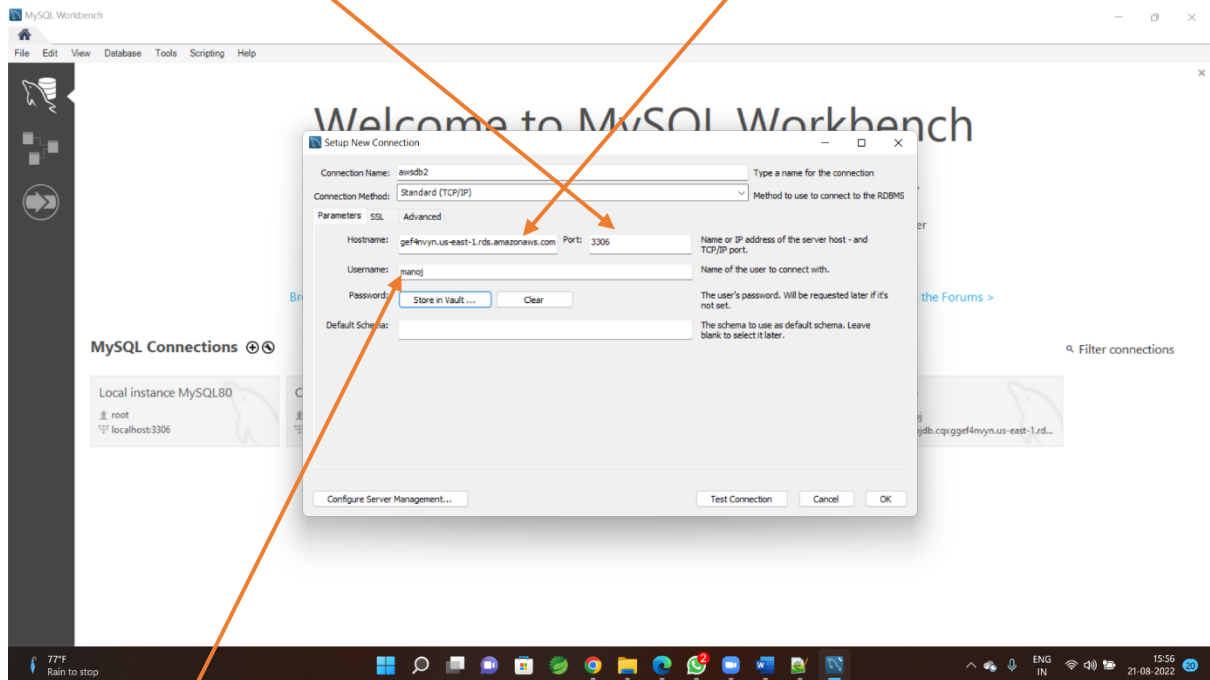
Step-4

open MySQL Workbench in your Laptop and click on + for new connection



Step-5

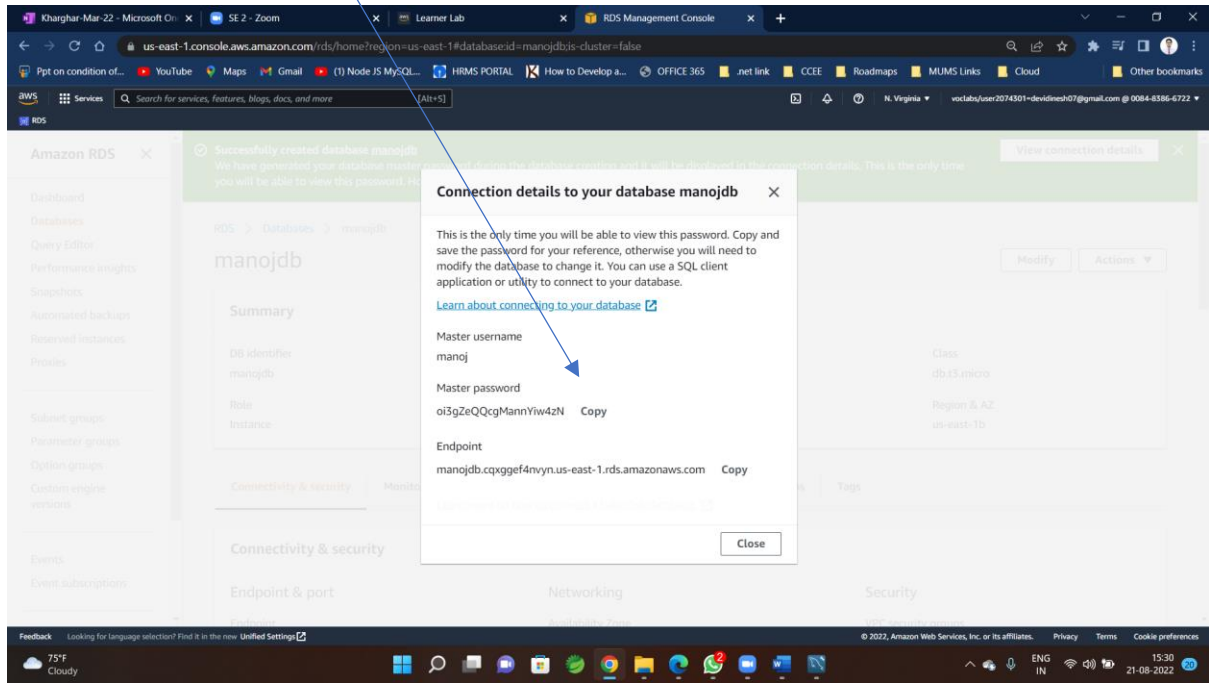
Paste Endpoint (from RDS details) in hostname keep port same



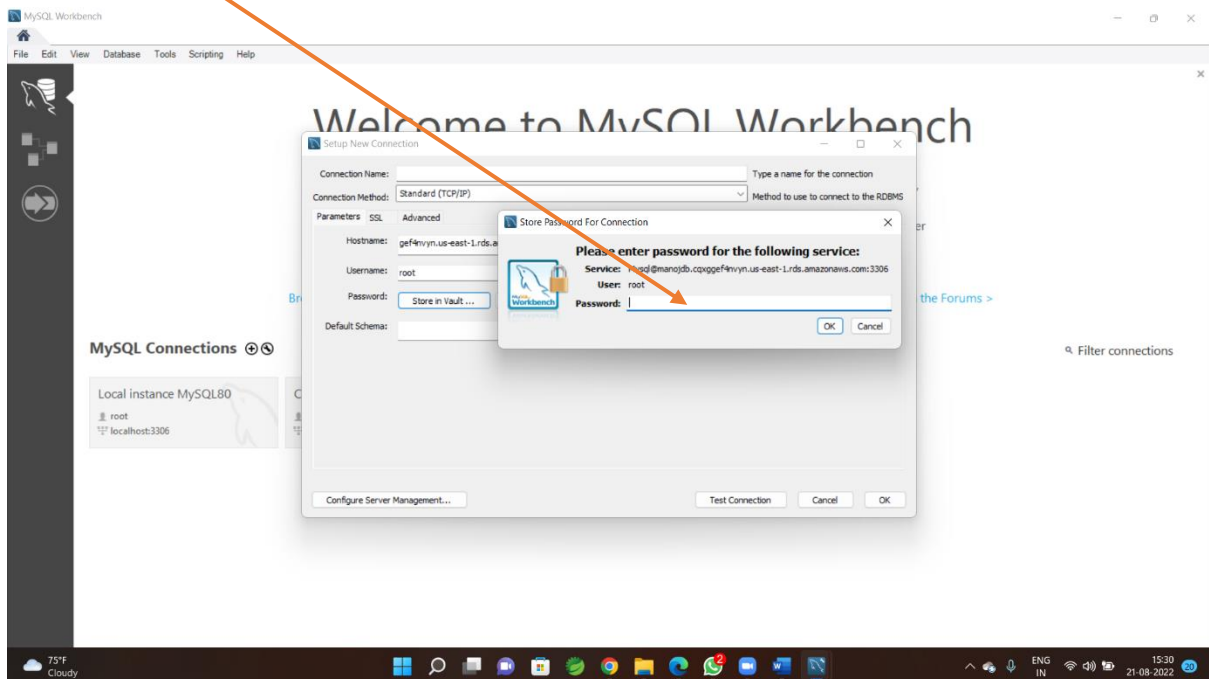
Give User name same as you given while creating RDS

Step-6

copy Password from here

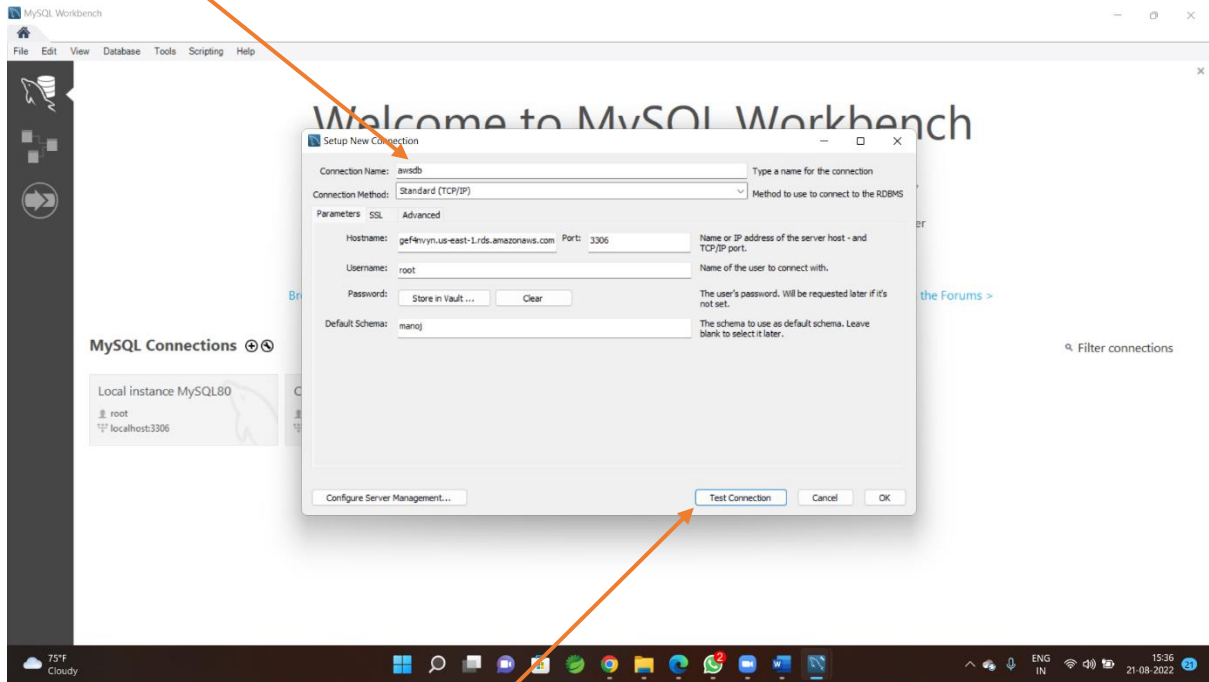


and paste in MySQL To here



Step-7

Enter connection name (any of your choice)

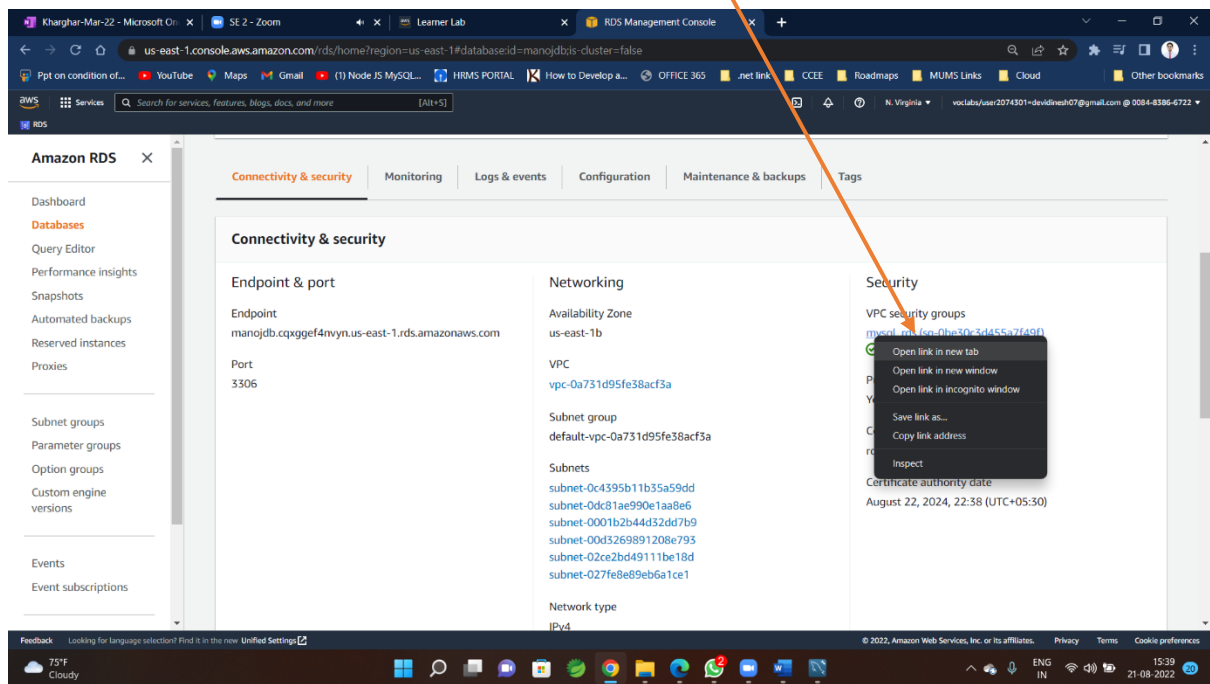


Now click on Test Connection

Step-8

If test fails check security group

Right click and open in new tab



Step-9

In new window of security group of RDS

securitygroup → Click on → inbound Rules → Edit Inbound rule

The screenshot shows the AWS Management Console interface for RDS Security Groups. The left sidebar contains navigation options like EC2 Dashboard, Events, Tags, Limits, Instances, Images, and Elastic Block Store. The main content area shows the 'Security Groups (1/1)' page. A table lists the security groups, with one selected. Below the table, the 'Inbound rules' tab is active, showing a single inbound rule. An arrow points from the 'Edit inbound rules' button to the 'Edit inbound rule' text in the instructions above.

Name	Security group...	Security grou...	VPC ID	Description	Owner	Inbound rule...	Outbound rules count
-	sg-0be30c3d455a7f49f	mysql_rds	vpc-0a731d95fe38...	Created by RDS ...	008483866722	1 Permission entry	1 Permission entry

sg-0be30c3d455a7f49f - mysql_rds

Details | **Inbound rules** | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

Inbound rules (1/1)

Name	Security grou...	IP version	Type	Protocol	Port range	Source	Description
-	sg-05b585df91...	IPv4	MySQL/Aurora	TCP	3306	27.97.72.34/32	-

Manage tags | [Edit inbound rules](#)

Step-10

Make it Public

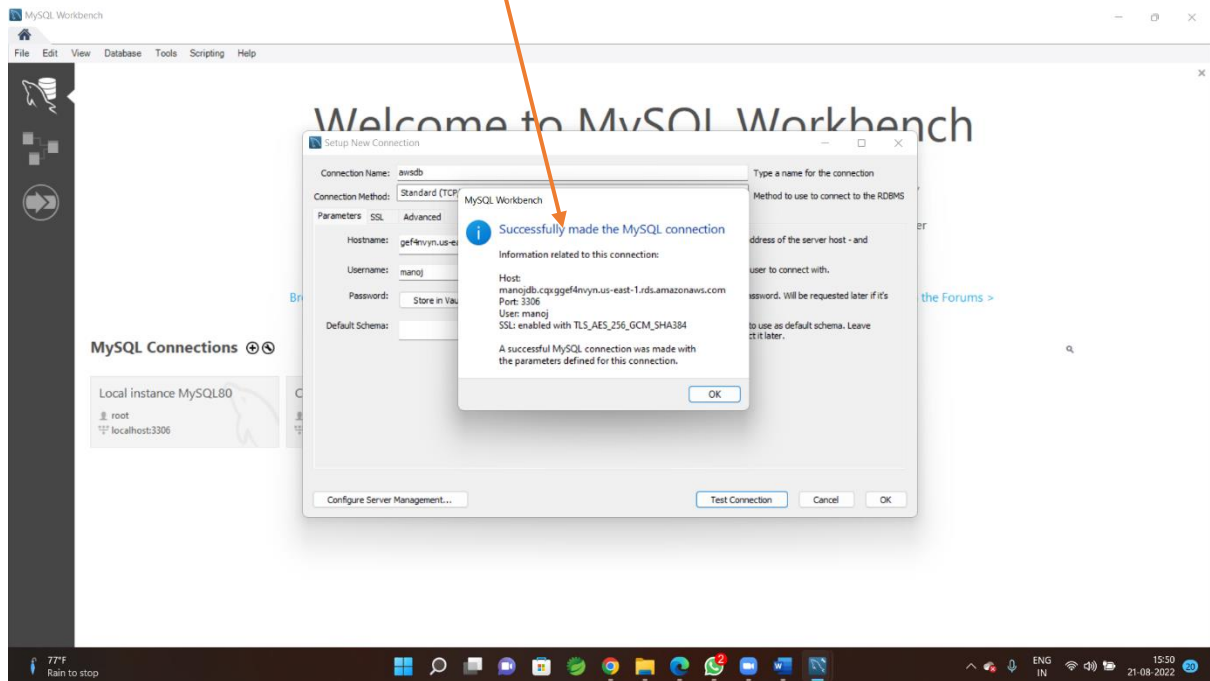
The screenshot shows the AWS Management Console interface for editing inbound rules on a security group. The browser address bar indicates the URL: `us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-0be30c3d455a7149f`. The page title is "Edit inbound rules" with a sub-header "Inbound rules control the incoming traffic that's allowed to reach the instance."

The "Inbound rules" table has the following columns: Security group rule ID, Type, Protocol, Port range, Source, and Description - optional. The table contains one rule with ID `sg-05b585df91ea20474`, Type `MySQL/Aurora`, Protocol `TCP`, and Port range `3306`. The Source field is open, showing a dropdown menu with options: Anywhere..., Custom, Anywhere-IPv4, Anywh..., Anywh..., and My IP. The `Anywhere-IPv4` option is highlighted, and the text "Anywhere-IPv4" is visible in a tooltip. The "Add rule" button is visible below the table. At the bottom right of the table, there are buttons for "Cancel", "Preview changes", and "Save rules".

The Windows taskbar at the bottom shows the system clock as 15:44 on 21-08-2022, with a weather widget indicating 75°F and Cloudy.

Step-11

Successful connection



Step-12

Create and use

