TD SYNNEX

Relational Database Service in AWS Version 2.0

Step by Step Guide

The information below includes detailed pre-deployment requirements, an in depth step by step guide for the AWS RDS v2.0 Click to Run deployment, and post deployment steps that will need to be considered.

Relational Database Service v2.0 Pre-Requisites

✓ Infrastructure Requirements (skip those steps if you are creating a new VPC together with the RDS instance)

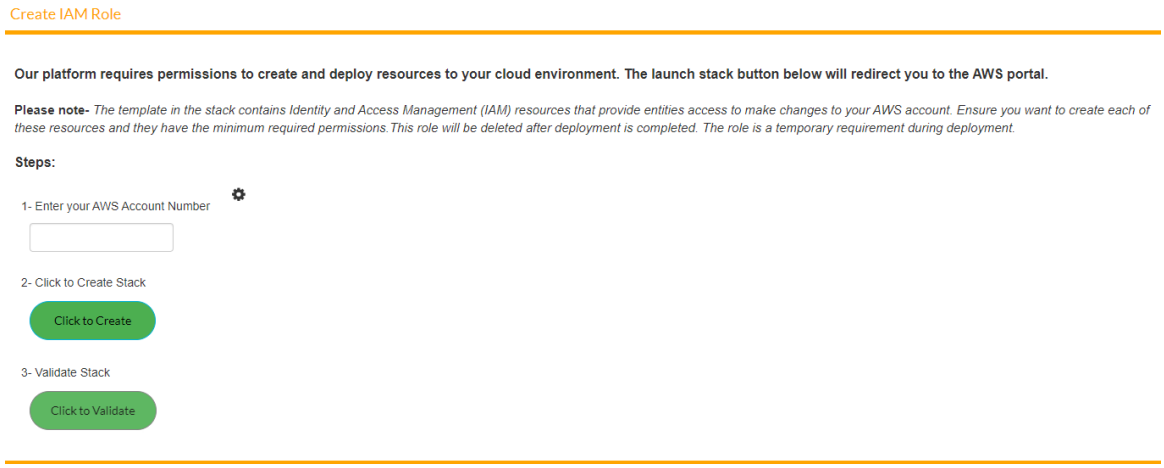
• ***Existing VPC, Subnets and Subnet Group(optional)*** **-** This is a requirement only if the user decides to use an existing VPC. A new set of VPC, Subnets and a Subnet Group can be provisioned together with the RDS if the client buying the solution chooses so and has available quota in the selected region. A VPC with associated subnets must already exist in the region, with corresponding route tables, gateways etc. Also if the VPC has an subnet group that is ready to use it can be selected from a drop down. The solution does not do any configuration outside of the scope of provisioning RDS based resources, so to ensure connectivity the VPC must be configured properly. At least two subnets in different AZ's in the same VPC need to be joined into a Subnet Group where the RDS instance will be placed

• ***Existing VPC Security Groups(optional)*** **-** This is optional and can be provided only if the user decides to use an existing VPC. If the client buying this solution decides not to provide at least one Security Groups access to the RDS instance will be very limited and the default VPC Security Group will be attached, but the connectivity also can be set up manually after the deployment is finished. If the user chooses to create a new VPC together with the provisioning of the RDS instance only a default Security group with no external traffic permissions will be created and attached to the instance, because the VPC at its creation stage will not include any components able to query the database.

Relational Database Service v2.0 Pre-Deployment Steps

1. In case the user decides to deploy to an existing VPC he needs to make sure the VPC is created and has at least two subnets in different Availability Zones, an own subnet group can be also provided or created automatically during the deployment. Security groups can also be pre-defined if the person buying the solution already knows the origin from where the traffic will be sent. If the solution is deployed into a new VPC this step is not required.

2. When the user starts the purchasing process he will be sent to the Role creation page. This creates a temporal permission set that allows resource creation inside his AWS account. The least-privilege concept is applied here and this role will be deleted automatically after a successful deployment. The user must have his AWS credentials and the MFA device at hand (if two-factor authentication is used). This step is always required



Once the role is created and validated the deployment can start

3. Each AWS account has a specific amount of limits on how many of each resource is allowed per region. Those limits are known as quotas, and many of them are “soft limits”, meaning they can be increased by contacting AWS. The following resources need to have available quota before deployment is started. If the requirements are not met the user can either delete old objects in his account, chose another AWS Region or ask AWS for a soft limit increase

Resource	Default quota
Cloud trails (always deployed to us-east-1)	5
Number of VPCs per region (if creating a new VPC)	5
DB instances	40
DB subnet groups	50

Solution Overview:

"Amazon Relational Database Service, or RDS, is a distributed relational database service solution optimized to run in the AWS cloud. Administration processes like patching the database software, backing up databases and enabling point-in-time-recovery are managed automatically. AWS does not offer an SSH connection to the underlying virtual machine as part of the managed service. There is a variety of optimizations and shirt sizes to choose from, so the instance type that best adapts to your use case can be selected."

Parameters & Inputs (a more detailed overview is shown on the next pages):

- Choose between deploying into existing VPC or creating a new one
- Select instance optimization (memory, burstable)
- Select the size of your instance (small, medium, large)
- Enable/disable Multi Availability Zone deployment
- Select an engine type(currently MySQL, PostgreSQL or MariaDB)
- Input the size of the root volume - default 5GB
- Input a name for your RDS instance
- Input the name of the database
- Input the database Admin user name
- Input the database Admin user password

• Select one of your VPC's you have in the dropdown from the selected region (existing VPC option only)

• Choose if you want to use an existing Subnet Group or create a new one inside the selected VPC (existing VPC option only)

• Select one of the Subnet Groups ID's used to the RDS instance from a drop down – If none were found you will receive an error message to create one first. (Use existing Subnet Group option only)

• Select two of the Subnet ID's used to create a Subnet Group from a drop down (Create New Subnet Group option only)

• Select the Security Groups ID's attached to the RDS instance – multiple ones can be selected, a button will appear in case the user wants to start over (optional, existing VPC option only)

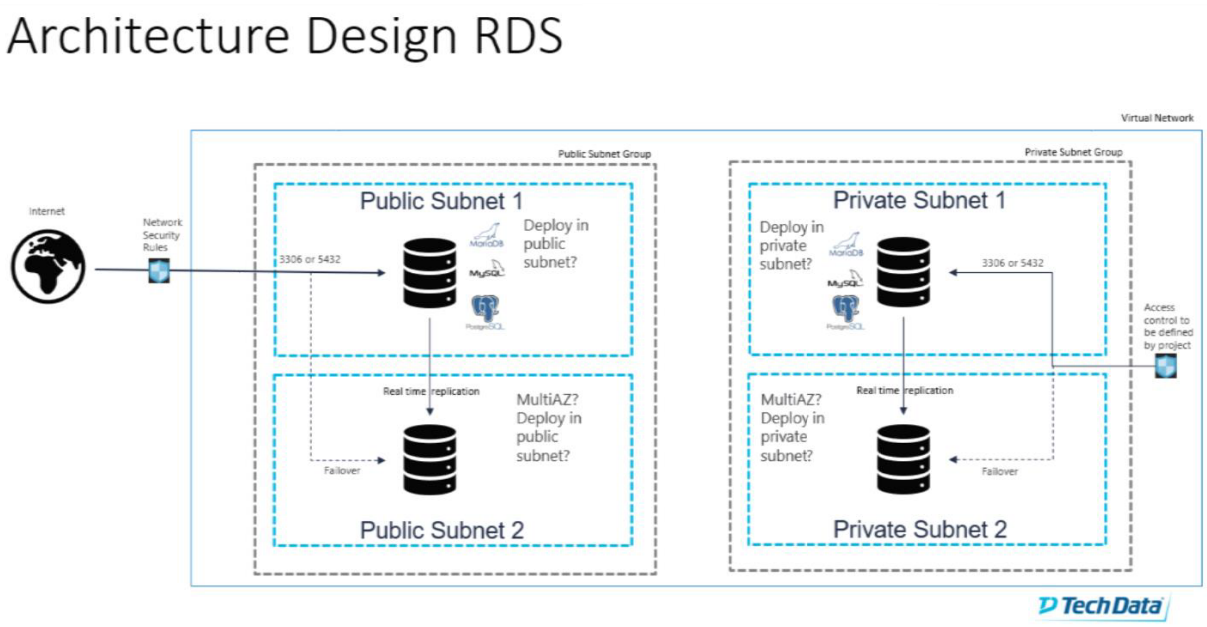
• Select to deploy into private or public subnets (new VPC only)

• Select two Availability Zones the subnets will be created in from the drop downs (new VPC only)

• Enter a CIDR block to use in the VPC and input CIDR blocks for each corresponding subnet (new VPC only)

• Select to create private or public subnets (new VPC option only)

Deployment Architecture:



AWS RDS v2 Click to Run Deployment

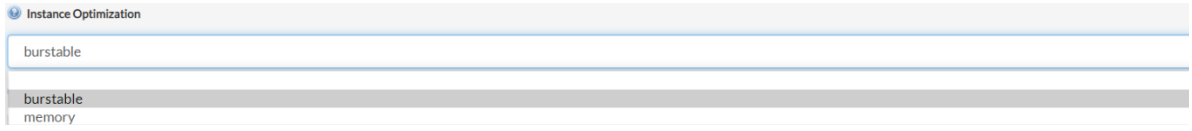
AWS RDS v2 Deployment and Considerations

Purchase the AWS RDS v2 Click to Run Solution through StreamOne Marketplace and proceed to the Digital Locker to configure and deploy the solution.

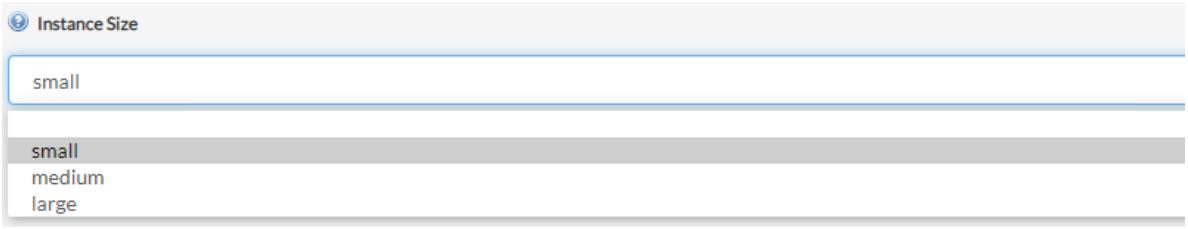
1. Select an available AWS Region: This is the region where the solution will be deployed. Some regions need to be enabled first on the target account before deploying to them, a warning message will appear in such case.

2. Select where to deploy the RDS instance: This option is to choose if the instance will be deployed to an existing or if a new VPC needs to be created, different fields will appear below depending on the choice made – steps 11-15 are for the first and 16-19 for the second scenario

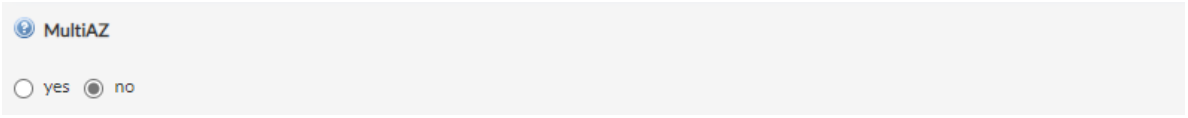
3. Select the instance Optimization: This option is used to select the performance to price balance of the EC2 instances hosting the database.



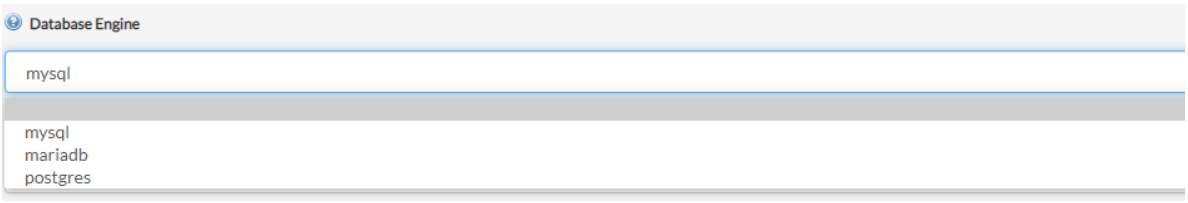
4. Select an instance Size: This option is used to choose the shirt size of the installation offering small sizes for test/dev environments and larger options for production workloads.



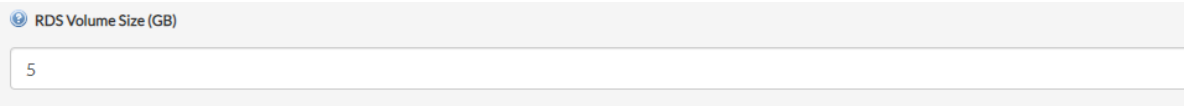
5. Enable/disable MultiAZ deployment: This option is used to set up High Availability. A passive identical copy of the Database will be kept in the second AZ of the Subnet Group and automatic failover will trigger once the main Database goes down or gets restarted. This is recommended for production databases.



6. Select Database Engine: Select one of the available engines.



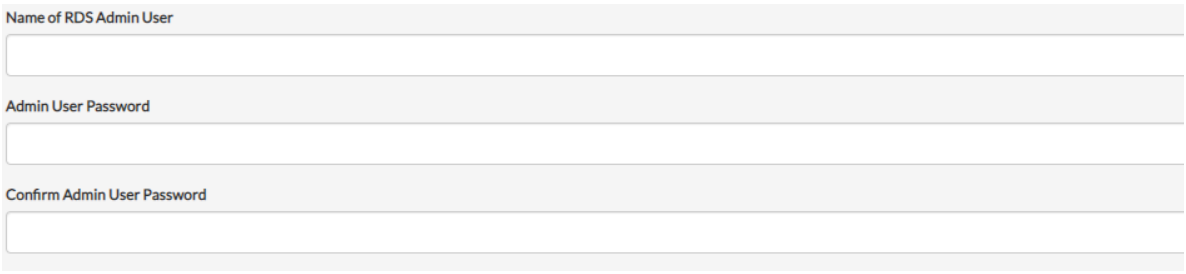
7. Select Database Volume Size: Select how much storage will be added to the instance.



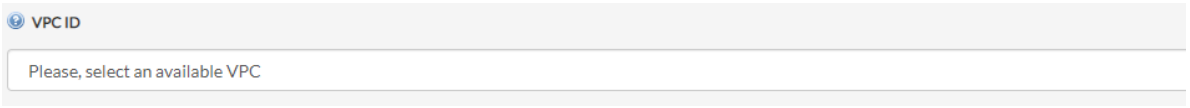
8. Name your RDS Instance:

9. Give your Database a Name:

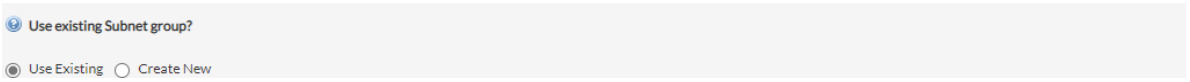
10. Create your Database Admin user and set a password: Since you cannot SSH/ RDP to your instance you will have to use those credentials to make your first connection programmatically using your favorite database client or tool.



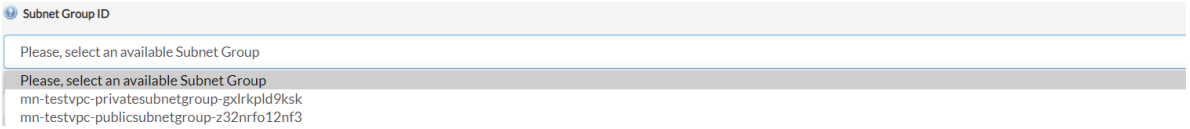
11. If deploying to an existing VPC the VPC ID is needed to know which sub-resources to retrieve in the next steps:



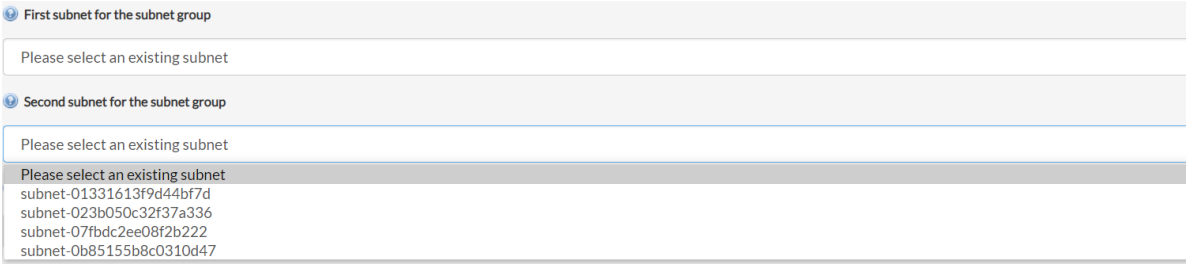
12. If deploying to an existing Subnet Group that is inside the selected VPC you can select “Use Existing” otherwise use the “Create New” option(recommended):



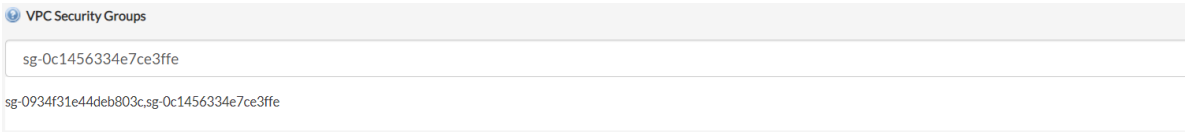
13. If deploying to an existing Subnet Group a dropdown will show a list of available Subnet Groups: The user has to make sure the selected group is compatible with an RDS deployment – it needs to have at least two subnets in two different Availability zones.



14. If Creating a new Subnet Group a list of available subnets from the selected VPC will be shown in two drop downs, the user needs to select exactly two subnets: Live validations will check if the two selected subnets are compatible, and an error message will warn the user in case of any issues encountered.

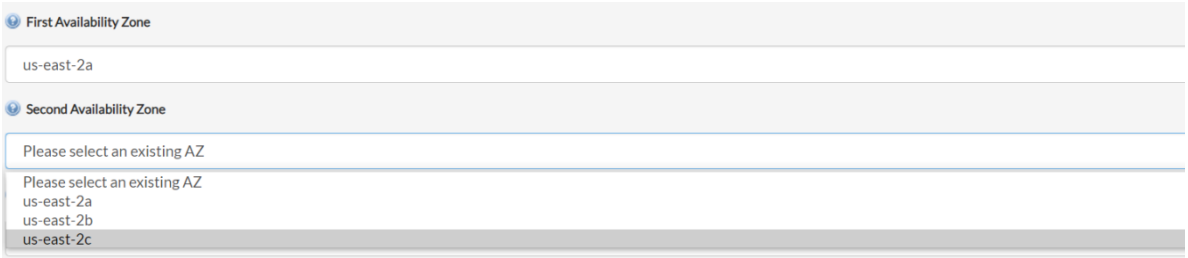


15. A List of VPC Security Groups will be shown and the user can choose one or more to attach to the RDS instance: This is completely optional, however if no Security Group gets selected Amazon will automatically use the default VPC Security Group. The “Clear” button is used to reset the selection and start over.

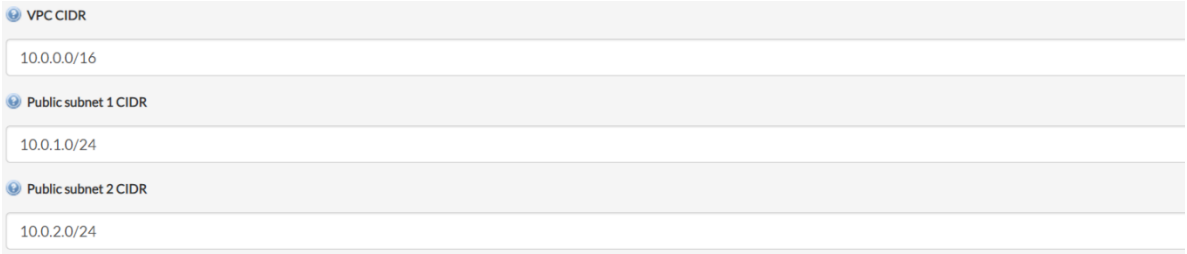


16. If creating a new VPC select if the Database will be inside private or public subnets: Some additional information will be required so the scripts know what kind of configuration will be put into the VPC. The recommendation is to have the RDS instance always in a private subnet – the default values are designed to deliver such a secure environment.

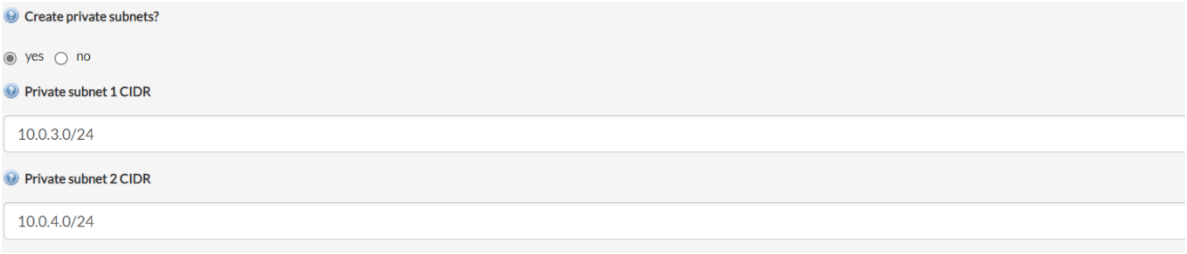
17. Select exactly two Availability Zones to create a Subnet Group: Two drop downs will show a list of available Zones inside the selected region. Live validations will check if the two selected AZ’s are compatible, and an error message will warn the user in case of any issues encountered.



18. Configure IP ranges for the VPC and subnets: Must be valid CIDR blocks, the user can use the pre-populated values.



19. Do the same as above for private subnets (if used):



20. Review your configuration and press “Deploy Now”

---------- Proceed to the next page to for post-deployment steps ----------

Post-Deployment activities for AWS RDS v2:

• Verifying the state of your instance.

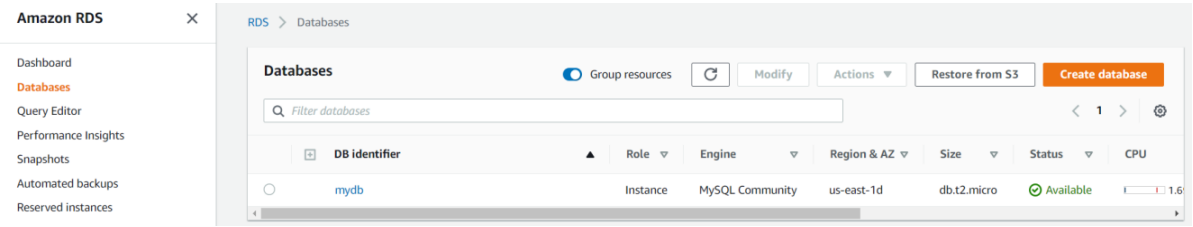
• Connecting to your database.

• Modifying network access permissions.

Post Deployment Activities

Verifying the state of your instance.

When the instance is first deployed, its state will change to “running” after some minutes. If the instance doesn’t start there might have been a problem during startup, so either check the deployment logs or contact our support. To verify the state, go to your AWS console. Once logged in, select the service “RDS”. Go to “Databases”. Your instance should appear there, with the name you selected as “RDS Instance ID”. The state will be displayed in the “status” column.



Connecting to your Database.

At some point you will have to connect to your RDS instance, for example to add users, tables, additional databases, etc. You cannot SSH to the instance hosting the RDS so the only way to access it is through a database client. Make sure the client is connected from a location that has access to it like an EC2 instance inside the same VPC, on premise machine accessing via a tunneled connection through a bastion host, etc. Opening the database ports to the entire internet even with IP filtering is a bad practice and should be avoided.

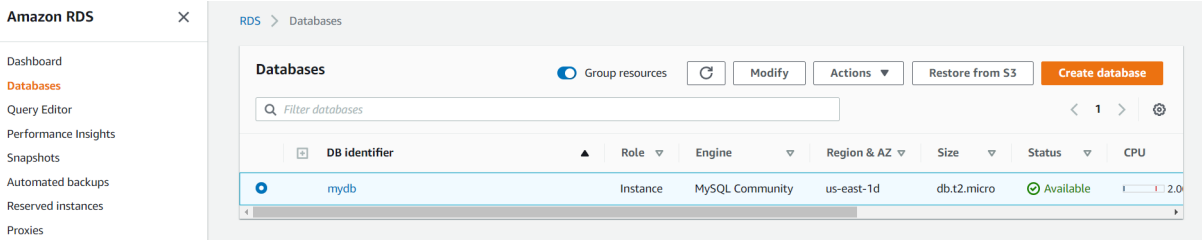
Modifying network access permissions.

It is possible that the basic permissions issued at instance deployment will need to be modified later on as demands change, or it could be that a mistake was made and the proper CIDR block was not assigned. To modify the network access permissions, follow these steps:

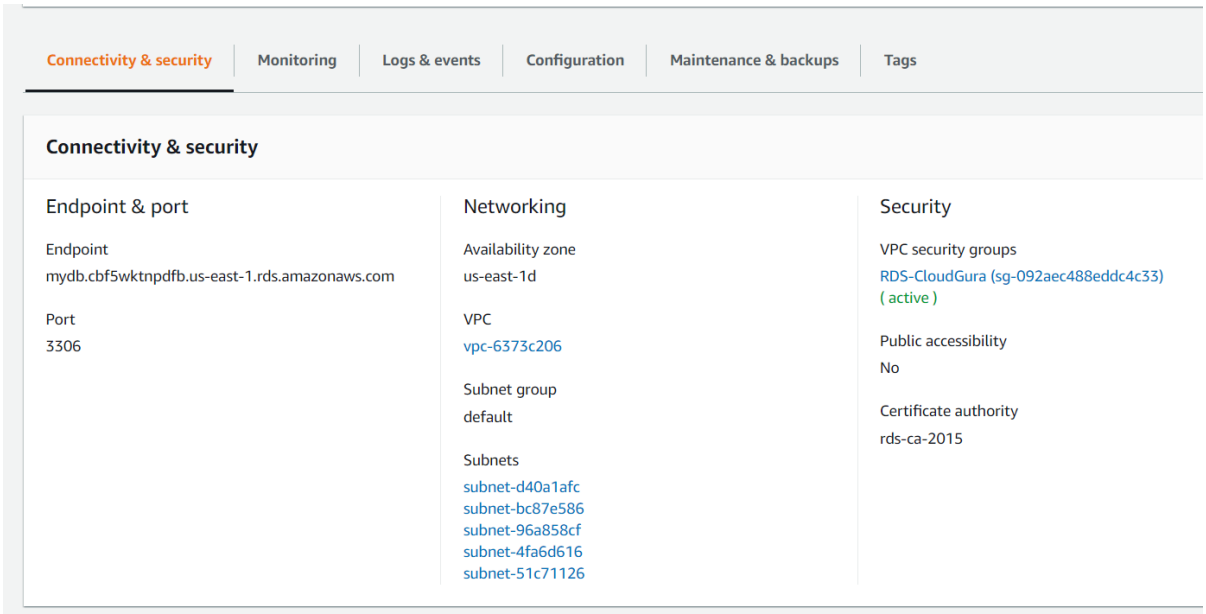
1. Connect to your AWS console. Select the service “RDS”.

2. Go to “databases” in the left navigation bar.

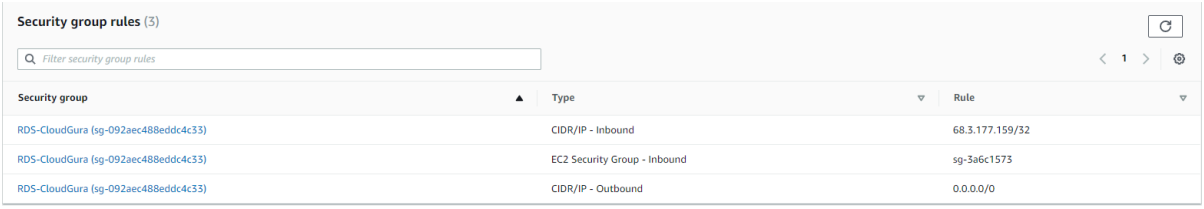
3. Select your instance:



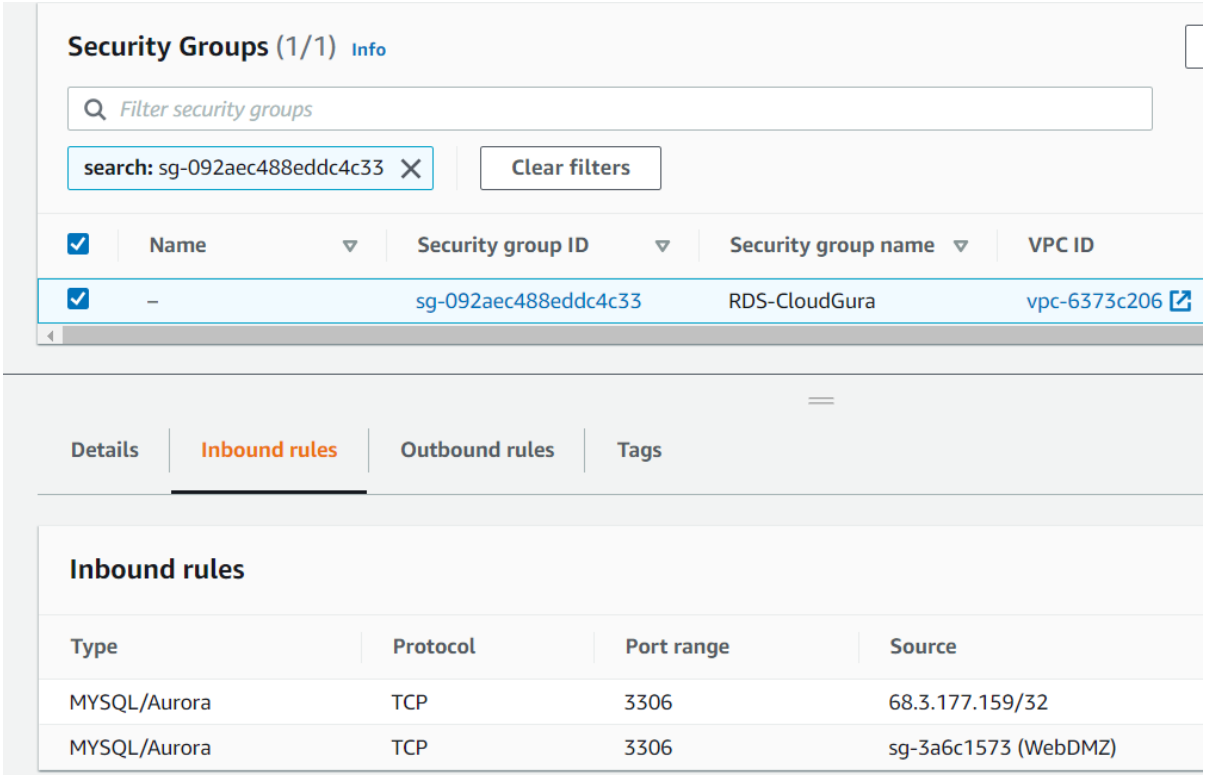
4. On the bottom half, select the “Connectivity & Security” tab:



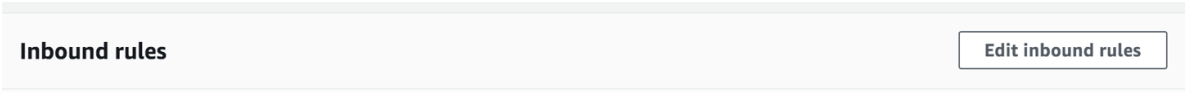
5. In the “Security group rules” section, review the applied rules and select the Security Group you want to change. You can also Modify your database settings to add or remove additional Security Groups.



6. You will be taken to the “Security Groups” interface which is under “EC2”. There, scroll down until you see the “Inbound rules” section. Your access rules should be displayed there. If you selected “MYSQL/Aurora”, a rule to port 3306 will be displayed there, from the IP address or security group ID that you selected:



7. To modify or add access rules, click on “Edit inbound rules”, in the top right corner of the “inbound rules” section.



8. You will be able to modify the “source” and well as the port, or add additional ports. Remember that it is possible that you will have to edit the Security Groups assigned to the subnet to allow access to the host.